Contract for Work
for
the Delivery and Installation of
A QUEUE MANAGEMENT AND PASSENGER FLOW MONITORING SYSTEM

Client's filing number:
0227011248

Contractor's filing number:

CONTRACT FOR WORK FOR THE DELIVERY AND INSTALLATION OF A QUEUE MANAGEMENT AND PASSENGER FLOW MONITORING SYSTEM

(HEREINAFTER THE "**CONTRACT**")

The Parties:

Letiště Praha, a. s.
With its registered office at: K Letišti 1019/6, Praha 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**")

Xovis AG
With its registered office: Industriestrasse 1, 3052 Zollikofen, Switzerland
registered and kept in the Commercial Register of canton Bern

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 the **"Parties"** or individually as a **"Party".**

Preamble

Whereas:

(A) The Contractor is interested in delivering and installing for the Client a queue management and passenger flow measuring system as defined below in this Contract, and

(B) The Client is interested in purchasing a queue management and passenger flow measuring system from the Contractor,

The Parties have agreed, on the day, month and year below, as follows:

1. DEFINITIONS AND INTERPRETATIONS

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

1.2 "**Author's Work**" means any result of the Contractor's activity created while carrying out modifications under this Contract, which shows the characteristics of a work protected under the Copyright Act.

1.3 The "**Price**" has the meaning set forth in Art. **12.1** hereof.

1.4 "**Documentation**" means the following documents related to the Performance:

1.4.1 certificates and declarations of conformity for each type of Hardware,

1.4.2 Manufacturer's original documentation for the Queue and Passenger Flow Management System, including a communication diagram,

1.4.3 instructions for use,

1.4.4 documentation of the actual state of the new connection of the System, in digital form, which is specified in Annex 1 hereto,

1.4.5 certificates of warranty for the Hardware.

1.5 "**Hardware**" means the equipment forming part of the Queue Management and Passenger Flow Monitoring System as defined in Annex 1 to this Contract and in the Procurement Documents.

1.6 "**Customisation**" means adapting the Queue and Passenger Flow Measuring System to the specific needs of the Client, in particular by setting custom parameters and in accordance with the Client's instructions.

1.7 "**Integration**" means the material and functional interconnection of the Hardware with the Client's other software and/or hardware.

1.8 "**Installation**" means (i) the phased performance of all activities necessary to make the Queue and Passenger Flow Measuring System operational, including but not limited to installation, attachment and connection of the Hardware to the electricity and data network at a location to be determined by the Client and interconnection of the Hardware with other hardware assets within the System (ii), in the case of Software, the performance of all activities necessary to make it operational on a cloud-based platform provided by the Contractor.

1.9 "**Licence**" means a right and licence for the Client to access and use the Software for the duration of the Contract.

1.10 "**Place of Performance**" has the meaning set forth in Art. **4.1** hereof.

1.11 "**Regulation**" means 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).

1.12 "**Civil Code**" means Act No. 89/2012 Coll., the Civil Code, as amended.

1.13 „**Moment of Acceptance**" means the day of signing the Handover Report relating to the Performance and any parts thereof (phases) delivered under this Contract.

1.14 "**Verification Operation**" means the period of fourteen (14) calendar days unless another period is agreed on between the Parties, counted from the Contractor's invitation issued after the completion of the Installation of each phase under **Annex 3** hereto (in the case of phase 1 after the conclusion hereof) and after the Integration during which (i) the delivered Hardware and Software which has been made available, scheduled for that particular phase pursuant to **Annex 3** hereto, will be tested in the Client's environment, under the Client's technical conditions and using actual data, (ii) the properties of the delivered Performance will be verified according to the Documentation handed over, and (iii) the functionality of the delivered Performance will be tested. As part of the Verification Operation, the Client will also be entitled to verify compliance of the delivered Performance with the security requirements specified in Annex 4 hereto.

1.15 "**Performance**" has the meaning set forth in Art. **2.1** hereof.

1.16 "**Working 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.

1.17 "**Intellectual property rights**" mean 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.

1.18 "**Handover Report**" means the paper or electronic report on the handover and acceptance of the Performance or parts thereof (depending on the specific phase) signed by both Parties.

1.19 "**Contract for Provision of Services**" means the contract for the provision of services, spare parts and general modifications for the System, entered into between the Contractor and the Client together with this Contract filing number 0227011249.

1.20 "**Software**" means a third party software applications and/or Software-as-a-Service application specified in more detail in **Annex 1** hereto, 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** Functional and Technical Specification of the Queue Management System to this Contract.

1.21 "**System**" means the Hardware including Software designed to measure queues and passenger flows, also referred to as the "**Queue Monitoring System**" or "**QMS**", 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, as specified in **Annex 1** hereto and in the Procurement Documents.

1.22 "**Technical Specification**" means the functional and technical specification of the System which forms part of this Contract as its **Annex 1**.

1.23 "**Upgrade**" means the provision of new versions of the Software, particularly with extended functionality.

1.24 "**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.

1.25 **"Defect"** means (i) legal defects of the Performance or (ii) discrepancy between the actual properties of the Performance and the properties set forth in this Contract or in the Documentation or in the Technical and Functional Specification of the Performance pursuant to **Annex 1** hereto, or (iii) any functional deviation of the Performance from the standard functional properties described in the Contract or in the Documentation or in the Technical and Functional Specification of the Performance pursuant to **Annex 1** hereto, which negatively affects its operation or functionality.

1.26 The "**Category A Defect**" means the most severe Defect manifested by the fact that:

1.26.1 the delivered Performance has legal defects, or

1.26.2 the Performance or any part thereof is completely non-functional or the Client cannot use the Performance or any part thereof, or

1.26.3 the delivered Performance 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 each individual location installed,

1.26.4 the Performance causes non-functionality of the System or part thereof.

To avoid any doubt, the Parties have agreed that a Category A defect (other than a defect under Article 1.28.1 of the Contract) will include an overall non-functionality of the Software and/or Hardware of more than 50% of the measured area – assessed for each individual location separately and/or the System does not provide the required data or does not provide it in the required quality (accuracy), preventing the use of the System.

1.27 "**Category B Defect**" means a Defect manifested by the fact that the use or functionality of the Performance or any part thereof, or the functioning of the System, 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 – assessed for each location individually unless it is a Category C Defect.

1.28 "**Category C Defect**" means a Defect which

1.28.1 does not prevent or has minimum impact on the proper use or functionality of the Performance or any part thereof and/or of the System on the part of the Client, and

1.28.2 has minimum impact on the Client's processes.

1.29 "**Manufacturer**" means the manufacturer of the Hardware, i.e. the company Xovis AG and its authorised representatives.

1.30 "**Personal Data Processing Act**" means Act No. 110/2019 Coll., on the processing of personal data, as amended.

1.31 "**Penetration Testing**" means a proactive security evaluation methodology aimed at assessing the resilience of computer systems, networks, or web applications by simulating real-world cyber attacks. The primary goal of penetration testing is to uncover vulnerabilities in the target system's infrastructure, software, and security measures before malicious actors exploit them.

1.32 Other definitions. 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.

1.33 Interpretation.

1.33.1 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.

1.33.2 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.

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

2. SUBJECT MATTER OF THE CONTRACT

2.1 Under the terms and conditions agreed to in this Contract, the Contractor undertakes to:

2.1.1 Perform the Installation and Integration of the System and Software Customisation according to **Annex 1** hereto,

2.1.2 provide the Client with the Licenses and right to use of the Software and the Documentation,

2.1.3 provide training to the Client's employees in the scope under Art. **3** hereof,

2.1.4 successfully complete the Verification Operation of each phase in accordance with **Annex 3** hereto.

2.2 Under the terms and conditions hereof, the Client agrees to accept the duly completed Performance referred to in Art. 2.1. of the Contract or any part thereof intended for separate delivery and to pay the Price for it under Art. 12 hereof.

3. TRAINING ON THE QUEUE MANAGEMENT SYSTEM

3.1 Under the terms and conditions agreed to in this Contract, the Contractor undertakes to:

3.1.1 **At least 10** business days prior to the commencement of the Verification Operation in the first phase at the Client's headquarters, provide initial training for end-users for 1-10 **persons** designated by the Client, whose job duties will include working with the user interface of the System, the content of which will be to master the operation of the user interface in its entirety.

3.1.2 to carry out training for at least **2 workers** (IT administrators) of the Client in the Place of Performance at the beginning of the Verification Operation, the content of which will be mastering the routine administration, maintenance, configuration and monitoring of the state of the system in the full extent, including instruction to manage the replacement of installed Hardware (measuring sensors).

3.2 The training fee under Art. 3.1 is part of the Price for the Performance but will be invoiced separately upon completion of the said training.

3.3 For purposes of this Contract, the delivery of the Queue Management System, including Hardware, Software, Installation, Integration, Customisation, provision of Licenses, and provision of training and upgrade training will hereinafter be referred to as "**Performance**" OR "**Work**".

4. TIME AND PLACE OF DELIVERY

4.1 The place of performance is the area of the Prague/Ruzyně international airport, Terminal 1 and Terminal 2 (hereinafter the "**Place of Performance**").

4.2 The Work will be executed during the operation of the airport, partially in its security restricted area while complying with the Client's operating rules and instructions. The execution of the Performance is fully subject to the operation of the airport and all Client's operating rules and instructions must be complied with during the execution. Based on a notification sent by the Client's operational unit, the execution of the Work in any given period determined by the Client may be moved to night hours (i.e. from 10:00 p.m. to 6:00 a.m.) or to non-working days.

4.3 The Contractor agrees to deliver the Performance and successfully complete the Verification Operation of all phases pursuant to **Annex 3** to this Contract no later than 9 (nine) **months** after receipt of the Client's written request to commence the phase 2 Installation.

5. TERMS AND CONDITIONS FOR EXECUTION OF THE WORK

5.1 The execution of the Performance is fully subject to the operation of Prague/Ruzyně Airport.

5.2 The Contractor is obliged to comply with all instructions given by the Prague/Ruzyně Airport operator which lead to ensuring the safe and smooth operation of the airport.

5.3 The Contractor is obliged to comply with the hygiene limits set out in Government Decree No. 272/2011 Coll., on the protection of health from adverse effects of noise and vibrations, as amended.

6. INSTALLATION PROCEDURE – QUEUE MANAGEMENT DEVICE

6.1 For the sake of the commencement of the Verification Operation and Penetration Testing, the Contractor agrees to hand over to the Client the part of the Work installed under the procurement procedure for the purpose of sample testing once this Contract has entered into force, where the successful outcome of such sample testing was a condition for the conclusion of the Contract. This part of the Work will be handed over by the Contractor to the Client upon successful completion of the Verification Operation and Penetration Testing already under this Contract and will become part of the QMS as Phase 1 and will be subject to the terms and conditions hereof.

6.2 The Contractor agrees to deliver each subsequent phase of the System, including the Installation and mounting of the delivered Hardware at the Place of Performance, always upon the Client's written request

and according to the anticipated phasing schedule provided in **Annex 3** hereto and to invite the Client to commence the Verification Operation of the relevant phase immediately after the completion of the Installation of that phase. Each phase will be ordered separately, and the proposed schedule phasing provided in **Annex 3** hereto is anticipated but not binding. The Client is entitled to order phases in any order and may invite the Contractor to start the implementation of the next phase even before the completion of the implementation of the previous phase.

6.3 The Client is responsible for bringing the interface of the required infrastructure to the point of installation of the required technology for the queue management device, except for Phase 4 where, if the technology is required to be installed at the roof structure of Terminal 2, the bringing of the infrastructure will be part of the installation provided by the Contractor.

7. RIGHTS AND OBLIGATIONS OF THE PARTIES

7.1 Rights and obligations of the Contractor relating to the Hardware

7.1.1 The Contractor agrees to deliver to the Client the Hardware which will be new, unused, undamaged, fully functional, in the highest quality provided by the Hardware Manufacturer, together with all rights necessary for its proper and undisturbed handling and use by the Client.

7.1.2 The Contractor declares that the delivered Hardware

7.1.2.1 meets the technical and functional parameters specified in **Annex 1** hereto.

7.1.2.2 is fully compatible with the System.

7.1.2.3 meets all requirements prescribed by the relevant legal regulations, in relation to hygiene, health and safety, technical and similar standards for the Hardware (hereinafter the "**Standards**").

7.1.2.4 is accompanied by all certificates and approvals necessary for its undisturbed and safe use.

7.1.2.5 is not encumbered with any third-party rights, including liens, and is free from any legal or factual defects.

7.1.3 Furthermore, the Contractor declares that undisturbed handling or use of the Hardware by the Client is not prevented by any legal regulations, Standards or third-party rights.

7.2 Rights and obligations of the Parties relating to the Performance in general:

7.2.1 The Contractor agrees to Implement and Customise the Software for the queue management system according to the individual phases described in **Annex 3** to this Contract upon the Client's request, to hand over the Documentation to the Client and to invite the Client to commence the Verification Operation of the individual phases according to **Annex 3** hereto.

7.2.2 The Contractor agrees to deliver the Hardware, install the delivered Hardware for queue management including making the Software available, Integration and Customisation in all phases described in **Annex 3** to this Contract no later than **nine (9) months** from the date of the Client's written request to commence the second phase of the Installation.

7.2.3 In order to ensure the full functionality of the System, the Contractor agrees to:

7.2.3.1 perform Installation of the Hardware, make the Software available in accordance with the Technical Specification of the Performance under **Annex 1** hereto so as to ensure that the Performance is functional without any Defects in the Client's environment,

7.2.3.2 Verification Operation.

7.2.4 The Contractor undertakes to deliver to the Client, together with the Performance, documents relating to the Performance, it being understood that these documents must be handed over to the Client in the Czech or English language and at least in the extent of documents which form part of the Documentation.

7.2.5 The Contractor undertakes 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.

7.2.6 The Contractor shall provide the Performance free from defects duly and in time using skill and care that can be expected from a competent communications and information technology services provider operating in the air transport industry.

7.3 Client' Obligations

7.3.1 The Client must provide the Contractor with necessary cooperation during the Installation, Integration and Customisation (if any).

7.4 Obligations of the Contractor when executing the Performance:

7.4.1 During the execution of the Performance, the Contractor is obliged to comply with all generally binding legal regulations and the Client's regulations in the area of waste management and to dispose of waste created when executing the Performance in accordance with the applicable legislation at its expense.

7.4.2 The Contractor is obliged to keep all prescribed records and to keep documents related to the subject matter of performance under this Contract for the entire term of the Contract and to subsequently archive them for at least **five (5) years**. This especially applies to documents in the area of occupational safety and health (OSH) and those documents resulting from the Client's internal standards with which the Contractor was demonstrably acquainted within the framework of the provided instructions.

7.4.3 If the Contractor performs works with an increased risk of fire (e.g. welding), it is obliged to notify the Client of this at least **three (3) Business Days** in advance and to request from the Client a written consent to perform such works. At the same time, the Contractor is obliged to ensure, in cooperation with the Client's fire department, fire protection while performing works.

7.4.4 Subject to where such damage is caused by the acts or omissions of the Client or the Client's other suppliers, the Contractor is responsible for any and all damage caused to the health, property and environment of its employees or their property during the performance of its activities or in connection with them as well as for the same damage which its employees or subcontractors' employees cause during the performance of their activities or in connection with them to third parties or the Client.

7.4.5 The Contractor declares that it is insured for an insured amount of at least **EUR 420,000 (in words: four hundred and twenty thousand euros)** for the case of general liability for damage caused during the execution of the Performance or in connection therewith to the Client and/or a third party. By signing the Contract, the Contractor also undertakes to maintain an insurance policy in the same or larger extent until the signing of the Handover Report. The Contractor undertakes, at any time, to provide the Client at its request, within **seven (7) Business Days**, with the proof of the duration of the insurance.

7.4.6 The Contractor undertakes to execute and complete the Performance under this Contract in a manner ensuring that the Client's activity and the functionality of its technical equipment affected by the Performance are disrupted as little as possible.

8. LICENCE

8.1 Pursuant to the Copyright Act, as amended, and the Civil Code, as amended, the Parties have agreed that the Software and its Updates and Upgrades, and computer programs created (if any) by the Contractor during the execution of the Work, the outputs, the Documentation and any other performance by the Contractor under the Contract that is subject to protection under the Copyright Act.

8.2 Contractor grants Client a licence to use third party Software and/or Software developed by Contractor during the execution of the Work (if any) without any limitation for the duration of this Contract.

8.3 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.

8.4 The Parties have agreed that the Client is not required to use the License and/or the right to use the Software.

8.5 The Contractor agrees that the Client may use the Software, including Updates and Upgrades, outcomes and the Documentation, to the extent specified in Article **2.10** hereof, 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 grant authorisation to use that Software to such.

8.5.1 Remuneration for the provision of Licenses and/or rights to use under Article **8** is included in the Price pursuant to Article **12.1** hereof.

9. HANDOVER AND ACCEPTANCE OF PERFORMANCE

9.1 The Acceptance Procedure, i.e. the Handover and Acceptance of a sub-part of the Performance will take place for each partial phase of the Performance separately based on the two milestones described below (with the exception of phase 1) having been met:

9.1.1 a Verificaton Operation, and

9.1.2 the signing of a Handover Report.

In the case of phase 1, the acceptance procedure will additionally include the Penetration Testing described below.

The overall acceptance of the Performance (except for refresher training) will take place at the time of acceptance of the last phase of the Performance pursuant to **Annex 3** hereto.

9.2 Once the Installation of a sub-part of the Performance has been completed, the Contractor will invite the Client in writing to commence a Verification Operation, a proposal for the testing scenario being part of such invitation.

9.3 In the case of phase 1 Performance, the Client must commence the Penetration Testing after this Contract has entered into force and only subsequently to commence the Verification Operation, with the Penetration Testing to be performed by a third party at the Client's expense. The Contractor must provide the Contracting Authority with all necessary assistance for the Penetration Testing. If the Penetration Testing report does not indicate deficiencies in the Medium, High, Critical or higher category (or their significant equivalents), the Contractor will invite the Client to commence Verification Operation, with such invitation to include a draft test scenario. The meaning of the categories of deficiencies are as follows:

A “Critical” category deficiency – discovered vulnerabilities of the System can be immediately exploited to completely compromise the System (gaining access to unprivileged files, controlling the domain/local administrator, gaining other user accounts, the possibility of permanently disabling the System, etc.)

A “High” category deficiency – discovered vulnerabilities of the System that, in combination with other vulnerabilities or practices, pose a high risk.

A “Medium” category deficiency – special conditions for the exploitation of these vulnerabilities must be met or their possible exploitation has a limited impact.

9.4 If the Penetration Testing report shows that the System has Deficiencies of the categories listed in Art. 9.3 hereof, the Contractor agrees to remedy the identified deficiencies and, upon their remedy, to invite the Client to commence the Penetration Testing again, provided that Art. 9.3 hereof applies mutatis mutandis. This process and subsequent troubleshooting will be repeated as long as the System continues to exhibit deficiencies in the categories listed in Art. 9.3 hereof, up to a maximum of two (2) times in thirty (30) days of the commencement of the first penetration testing. Repeat Penetration Testing will be performed at the Contractor’s expenses. If the Penetration Testing report shows that the System exhibits deficiencies of the categories listed in Art. 9.3 of this Contract even after the second repetition of the Penetration Testing, the Parties will commence negotiations on further progress in the performance of the Contract and the Client will be entitled to withdraw from the Contract with effect from the date of delivery of written notice to the Contractor.

9.5 The time limit for the commencement of the Verification Operation will be **ten (10) Business Days** after approval of the testing scenario by the Client, unless otherwise agreed between the Parties in writing. If carrying out of Installation and/or Implementation and/or Integration forms part of the Performance, the Contractor will carry them out no later than on the day preceding the day of commencement of the Trial Operation.

9.6 The Verification Operation will be performed by the Client in the presence of or with telephone support from the Contractor, within a period of **fourteen (14) days** from the Contractor’s request sent to the Client unless otherwise agreed between the Parties.

9.7 The Parties will write a record of the performed Verification Operation, which will be signed by the authorised persons of both Parties.

9.8 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 partial phase of the Performance and the Client will be obliged to accept the partial phase.

9.9 After the Parties draw up a record of the performed Verification Operation (9.7) and the Client checks and confirms the fulfilment of the acceptance criteria specified in Art. 9.8 hereof, the functionality of the features of the delivered Performance according to the submitted Documentation, and the completeness of the Documentation, the Parties undertake to sign the Handover Report and the completeness of the Documentation, the Parties undertake to sign the Handover Report. The Verification Operation will be successfully completed by both Parties signing the Handover Report. The Handover Report will contain a list of remaining Defects (if any) with a time limit for their removal, it being understood that if such time

limit is not agreed, it will be deemed to be **fourteen (14) Business Days** from the day on which the Handover Report was signed.

9.10 If it results from the record of the performed Verification Operation that the Performance does not meet the acceptance criteria specified in Art. 9.8 hereof, the Contractor undertakes to remove detected Defects and, after removing them, to invite the Client to commence the Verification Operation, Art. 9.8 hereof being applied *mutatis mutandis*. This process of the testing and subsequent removal of Defects will be repeated until the Contractor meets the acceptance criteria specified in Art. 9.8 hereof, but no more than twice (2x) and no later than within **60 (sixty) calendar days** after the delivery of the results of the first Verification Operation for the given location. If even after the second repeated Verification Operation the criteria specified in Article 9.8 hereof are not met, the Parties will enter into negotiations on further progress in the performance of the Contract.

10. WARRANTIES

10.1 The Contractor hereby assures the Client that, after the Performance is accepted by the Client and the remaining Defects (if any) detected during the acceptance of the Performance pursuant to Art. **9.6** hereof, are removed, the Performance will function in accordance with this Contract and the Documentation relating to the Performance.

10.2 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 Performance is free of any known viruses or malware that would prevent the Client from using the Performance or the System or that would cause that the Performance and/or the System stops functioning or that its functioning is limited or otherwise negatively impacted.

10.3 The Contractor hereby provides the Client with a warranty that neither the Performance nor any other performance by the Contractor under this Contract nor the use of the 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 Art. 10.3, 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 Performance which does not infringe on any third-party Intellectual Property Rights and to compensate the Client and/or the Controlled Entity for damage caused to the Client or the Controlled entity thereby, as well as for any non-material damage incurred by the Client and/or the Controlled Entity.

10.4 The warranty under Article **10.3** hereof will be provided for a period of **24 (twenty-four) months** from the signing of the Handover Report in respect of the Performance or part of the Performance.

10.5 The warranty provided by the Contractor pursuant to Art. **10.1** and/or **10.2** hereof will apply for the period of **24 (twenty-four) months** from the day on which the Handover Report concerning the Performance or part thereof was signed. If any of the assurances pursuant to Art. **10.1** and/or **10.2** hereof proves to be untrue during the period mentioned in the previous sentence, the Performance will be deemed to have Defects. The Contractor agrees to remove a Defect of the Performance within **15 (fifteen) Business Days** from the written notification of the Defect in the Place of Performance in one of the following manners:

10.5.1 by replacing the defective Hardware with new Hardware free from any defects, or

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

10.5.3 in cooperation with the Client using remote access or in person in the Place of Performance by removing the Defect of Integration prevents proper use of the Hardware and Software, or

10.5.4 by agreement of the Parties on a manner of solving the complaint other than those described in Art. **10.5.1**or **10.5.2** hereof. The Parties will conclude a written agreement on another manner of removing the Defect if it is agreed to.

10.6 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).

11. TRANSFER OF RIGHTS

11.1 The ownership right to the Hardware delivered under this Contract will pass to the Client at the moment of full payment of a sub-part of the Performance to which the Hardware relates by the Client.

11.2 The risk of damage to the Hardware delivered under this Contract will pass to the Client at the Moment of Acceptance of the Hardware by the Client.

11.3 The Client is entitled to use the Software made available from the Moment of Acceptance of the sub-part of the Performance to which the Software relates by the Client.

12. PRICE

12.1 [redacted]

12.2 [redacted]

12.3 [redacted]

13.

13.1 [redacted]

13.2 [redacted]

13.3 [redacted]

13.4 [redacted]

13.5 [redacted]

14. TERM OF THE CONTRACT

14.1 This Contract comes into force on the date on which it is signed by the last Party and takes effect on the date of publication in the Register of Contracts.

14.2 In addition to discharge, this Contract will cease to be valid and effective also:

14.2.1 by a written agreement of the Parties;

14.2.2 by Client's withdrawal with immediate effect.

14.3 The Client is entitled to withdraw from this Contract if the Contractor materially breaches its obligations under the Contract and fails to remedy the breach within **fifteen (15) calendar days** from delivery of the written notification of breach of the Contract. A material breach of obligations will mean in particular:

14.3.1 The Performance does not meet any of the requirements under Art. **7.1** and/or **7.2** hereof, and/or

14.3.2 There is a breach of the warranty specified in Art. **10.1** hereof, and/or

14.3.3 The Contractor has concluded a contract (contracts) with a subcontractor (subcontractors) for the execution of the entire Performance or assigns this Contract without the Client's consent.

14.4 The Contractor is entitled to withdraw from this Contract only if the Client is in default with payment of the Price (or part thereof) on the basis of the invoice and fails to remedy such breach within **ten (10) Business Days** from delivery of the Contractor's written notification of such breach. For the avoidance of doubts, the Contractor is not entitled to unilaterally terminate this Contract in a manner other than as specified in this Art. **14.44** hereof. The provisions of Article **14.55** hereof will not be affected thereby.

14.5 The Parties may agree on the termination of this Contract. The agreement on the termination of the Contract must be concluded in written form.

14.6 The Parties agree that the provisions of this Contract concerning Licences, intellectual property rights, jurisdiction, protection of information, limitation of liability, confidential information, trade secret, penalties and damages will remain valid and effective even after the termination of the Contract in any of the manners specified in the Contract or in applicable legal regulations.

14.7 Withdrawal from the Contract must be made in writing and must be delivered to the other Party. In the event of withdrawal, this Contract will cease to exist on the day of delivery of the written notice of withdrawal to the other Party.

15. PENALTIES. DAMAGES AND CONTRACTUAL LATE PAYMENT INTEREST

15.1 Contractual penalties and contractual late payment interest

15.1.1 If the Client fails to pay to the Contractor the amount invoiced pursuant to Art. **12.1** hereof within the agreed maturity period, the Contractor will be entitled to claim from the Client a contractual late payment interest in the amount of 0.02% (in words: two hundredths of a per cent) from the amount due for each day of default.

15.1.2 If the Contractor breaches its obligation to remove a Defect or Defects within the time limit for removal agreed in Art. **10.5** 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:

Defect category	Contractual Penalty
Category A Defect	0.5% of the amount corresponding to the price for a given phase under Art. **12.1** hereof for each day the Category A Defect remains
Category B Defect	0.3% of the amount corresponding to the price for a given phase under Art. **12.1** hereof for each commenced day the Category B Defect remains
Category C Defect	0.1% of the amount corresponding to the price for a given phase under Art. **12.1** hereof for each commenced day the Category C Defect remains

15.1.3 If the Contractor breaches

15.1.3.1 the obligation pursuant to Art. **4.3** hereof, the Client will be entitled to claim from the Contractor a contractual penalty in the amount of **0.1% (in words: one tenth of a per cent)** from the Price of the entire Work for each day of default or part thereof,

15.1.3.2 any of the obligations under Article **7.4** hereof, the Client is entitled to demand from the Contractor a contractual penalty of **EUR 42,000 (forty-two thousand euros)** for each detected case of violation.

15.1.3.3 any of the obligations specified in Art. 18.18 hereof and/or Annex 4 hereto, the Client is entitled to demand from the Contractor a contractual penalty of **EUR 820 (eight hundred and twenty euros)** for each detected case of violation.

15.2 Each Party is obliged to indemnify the other party for all damage caused to the other Party due to breach of any of the Party's obligations specified in this Contract. If the Client or Client's other contractors/suppliers acts or omissions cause an effect on these, the Contractor will be relieved from paying such penalty. Notwithstanding any such indemnity shall be limited to an amount equivalent to one and half times the Price of the entire Work 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.

15.3 The arrangement on contractual penalties or the imposition of a penalty for a breach of a contractual obligation by legal regulations will not affect the Client's right to claim damages in the full amount. If one circumstance leads to a breach of more Articles of the Contract and, therefore, an obligation should rise on the part of the Contractor to pay a contractual penalty pursuant to two or more provisions of the Contract, the Contractor is only obliged to pay the contractual penalty to the Client pursuant to that provision of the Contract under which the Client requested payment of the contractual penalty from the Contractor, even pursuant to a provision which imposes an obligation to pay a higher contractual penalty.

15.4 If the Contractor causes any non-material damage to the Client, it is obliged to redress it in the full amount.

15.5 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 the entire Work. For the purposes of this Art. the Price of the entire Work means the sum of Price of all phases of the Work.

16. PROTECTION OF INFORMATION AND PROTECTION OF PERSONAL DATA

16.1 The Parties have agreed that all information which they communicated to each other during the conclusion and performance of this Contract and which is expressly designated as confidential will remain secret based on their will (hereinafter the "**Confidential Information**"). For the avoidance of doubts, the Parties have agreed that they do not regard the text of the Contract itself as Confidential Information.

16.2 Furthermore, the Parties have agreed not to disclose Confidential Information to anyone and to take measures preventing third-party access to such Confidential Information. The provisions of the previous sentence do not apply to cases where:

16.2.1 the Parties' obligation herein is contrary to what is prescribed by law; and/or

16.2.2 such information is disclosed to persons who are legally bound to confidentiality; and/or

16.2.3 such information is disclosed by the Party to persons in which that Party has ownership interest as of the day of disclosure of such information; and/or

16.2.4 such information becomes publicly known or available in any manner other than by a breach of the obligations resulting from this Article.

16.3 When performing this Contract, the Parties undertake to proceed in accordance with the Regulation as well as with the Personal Data Processing Act.

16.4 The Parties may process personal data solely for the purpose of performing this Contract. If the Contractor processes personal data for 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 Personal Data Processing Act in relation to these personal data.

16.5 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 Personal Data Processing Act in relation to these personal data.

16.6 Furthermore, the Contractor undertakes 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 Personal Data Processing 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.

16.7 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.

16.8 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.

16.9 If the Contractor breaches the confidentiality obligation pursuant to Art. 16.2 or the obligations when processing personal data pursuant to Art. 16.4 to 16.6 hereof, the Contractor undertakes to pay to the Client a contractual penalty in the amount of EUR 20 000 (twenty thousand euros) for each individual breach.

17. CONTACT DETAILS

17.1 Any notification or document which is to be made in writing under this Contract may be delivered in person or sent by registered post, fax transmission and/or by email to the Party to which it is to be delivered to its contact information specified in **Annex 2** hereto.

17.2 Communication other than as specified in Art. **17.1** hereof can be sent by either Party to the other Party by email or fax to the contact information of the other Party.

17.3 Either Party is entitled to change its contact information by sending written notification to the other Party.

17.4 All notifications between the Parties will refer to the identification of this Contract used by both Parties (number of the Contract) which is stated on the first page of the Contract.

18. OTHER ARRANGEMENTS

18.1 Jurisdiction. This Contract and the relations resulting from the Contract will be governed by the legal regulations of the Czech Republic, particularly by the Civil Code.

18.2 Entirety of the Contract. This Contract and Contract for Provision of Services constitutes the entire agreement between the Parties concerning the subject matter of this Contract and replaces any previous agreement that concern the subject matter of this Contract, except for any agreements on maintaining confidentiality or on the confidential nature of information.

18.3 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.

18.4 Precontractual Liability. Each Party hereby declares that it has duly informed the other Party about all factual and legal circumstances about which it knew or should have known at the moment of the conclusion of the Contract and which are relevant for the conclusion of this Contract.

18.5 Practices and business customs of the Parties. 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.

18.6 Discharge of an obligation under the Contract. The Contractor waives the right to claim any discharge of an obligation under this Contract pursuant to Section 2000(2) of the Civil Code.

18.7 Performance by a third party. In the event of performance other than pecuniary performance, the Client is not obliged to accept any performance offered to it by a third party with the Contractor's consent.

18.8 Exclusion of Certain Provisions. The Parties exclude the application of the following provisions of the Civil Code to this Contract: Section 557 (contra proferentem rule), Section 1740(3) (qualified acceptance of an offer), Sections 1799 and 1800 (clauses in adhesion contracts) and Section 1805(2) (prohibition of ultra duplum).

18.9 The Client expressly pointed out to the Contractor prior to the conclusion of the Contract that none of the paragraphs or sections of the Contract, its annexes and other parts is of an insignificant nature, the contractual regulation in the text of the Contract itself is not necessarily comprehensive and that the paragraphs and sections of the Contract, its annexes and other parts may contain provisions that could be regarded as surprising. The Contractor, as an entrepreneur-professional, declares that it took such information from the Client into account and that it has thoroughly acquainted itself with the Contract, all its annexes and other parts prior to the conclusion of the Contract.

18.10 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 within30 (thirty) 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.

18.11 Severability Clause. Should any provision of this Contract be or become invalid, unenforceable or ineffective, such invalidity, unenforceability or ineffectiveness will not affect the remaining provisions of the Contract. The Parties undertake to replace an invalid, unenforceable or ineffective provision within **five (5) Business Days** after the delivery of one Party's invitation to the other Party with a valid, enforceable and effective provision whose wording will correspond with the intent expressed by the original provision and by this Contract as a whole.

18.12 The Parties declare that pricing-related information contained in this Contract and its annexes, including but not limited to unit prices, discount structures, payment terms, and volume-based conditions, constitutes trade secret within the meaning of Section 504 of the Civil Code. The Parties undertake to maintain strict confidentiality of such information and ensure it is disclosed only to those 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 shall not be considered trade secrets unless explicitly specified otherwise.

18.13 Assignment, pledging and set-off. The Parties have expressly agreed that without the Client's prior written consent:

18.13.1 the Contractor is not entitled to assign any of its receivables from the Contract or any receivables created in connection with the Contract to a third party,

18.13.2 the Contractor is not entitled to pledge any of its receivables from the Client resulting from the Contract or any receivables created in connection with the Contract,

18.13.3 the Contractor is not entitled to set off, by a unilateral declaration, any of its receivables from the Client resulting from the Contract or any receivable created in connection with the Contract.

18.13.4 The Client is entitled to set off any of its receivables due from the Contractor under this Contract or that arises in connection with this Contract by unilateral declaration; this also applies to uncertain receivables.

18.14 Force majeure.

18.14.1 Neither Party will be in default with the fulfilment of its obligations resulting from the Contract due to the existence of a force majeure event, if such event makes the fulfilment of the obligations of that Party resulting from the Contract impossible. The immediately preceding sentence of this Paragraph will only apply for the duration of the existence of such force majeure event or for the duration of its consequences, and only in relation to the Party's obligation or obligations directly or immediately affected by such force majeure event.

18.14.2 A force majeure event will be deemed to be an event that the Party could not have foreseen at the time of conclusion of this Contract and/or is beyond the Party's control and which objectively prevents the Party from fulfilling its contractual obligations resulting from this Contract. Force majeure events include, in particular, war, embargoes, state or government interventions, terrorist acts, natural disasters, pandemics, failure of third-party service/hardware providers and networks and strikes by the Client's employees. For the avoidance of doubts, force majeure events do not include any instances of default with the fulfilment of obligations by the Contractor's Contractors or contractual partners towards the Contractor, strikes by employees of the Contractor and the Contractor's Contractors and contractual partners, as well as insolvency, overindebtedness, bankruptcy, settlement, liquidation or any other similar event concerning the Contractor or any of its Contractors or contractual partners, as well as execution against the property of the Contractor or any of its Contractors or contractual partners.

18.14.3 Should any force majeure event described in Art. **18.14.2** of this Contract occur, the Party on whose part the obstacle occurred will take all steps that can be reasonably requested from that Party which will lead to the restoration of normal activities in accordance with the Contract, as quickly as possible given the circumstances which caused that force majeure event. The Party agrees to inform the other Party about the occurrence of the force majeure event without undue delay as soon as such communication can be objectively made.

18.14.4 If the force majeure event lasts for more than **thirty (30) Business Days**, either Party will be entitled to withdraw from the Contract.

18.15 Limitation. The Contracting Parties prolong the duration of the limitation period with respect to all rights of the Client under the Contract to **15 years** from the day on which the right could have been first exercised.]

18.16 The Parties have expressly agreed that if this Contract is transferred to another entity as the legal successor of the Client in accordance with Act No. 125/2008 Coll., on transformations of commercial companies and cooperatives, as amended, also all Licenses will pass over to the Client's legal successor as of the effective date of such transfer without any further action. The Contractor hereby grants its consent to such transfer.

18.17 By signing this Contract, the Contractor

18.17.1 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"),

18.17.2 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"),

18.17.3 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,

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

18.17.5 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 Articles 18.17.1 to 18.17.4 of this Contract.

If during the term of this Contract, the Contractor discovers that the declarations under this Article are not true, or discovers that its subcontractors or sub-Contractors do not meet the conditions under this Article, it will inform the Client without delay. If the Contractor breaches any obligation under this Article and/or the Client discovers that the Contractor's representations under this Article are false and/or discovers that the sub-contractors or sub-Contractors do not comply with the terms of this Article, the Client will be entitled to withdraw from this Contract with effect from the date of delivery of the withdrawal to the Contractor.

18.18 The Contractor represent that it has read the Code of Conduct for Business Partners (hereinafter the "Code") on the www.prg.aero/ekop website. By signing this Contract, the Contractor agrees to comply with the Code during the performance hereof and to require the same from contractual partners who will participate in the performance hereof. The Parties agree that the Client is entitled to verify compliance with the obligations arising from the Code by the Contractor and its contractual partners who will participate in the performance of the Contract. The Contractor agrees to provide the Client with the necessary assistance for such verification, including on-site verification. If the Contractor fails to provide cooperation or if the Client discovers serious breaches of the Contractor's obligations under this Article of the Contract, the Client will be entitled to withdraw from the Contract with effect from the date of delivery of the withdrawal to the Contractor.

18.19 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 of the entire Work. 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.

19. FINAL PROVISIONS

19.1 Changes to the Contract. Acts changing the content of the legal relationship established by this Contract must be made in writing, (unless the Contract expressly provides otherwise) by means of amendments numbered in ascending order. Any changes to this provision of the Contract can only be made in writing by concluding an amendment to the Contract. For the purposes of this provision, any legal acts made using

electronic or other technical means which allow for the capturing of their content and identification of the acting person will not be regarded as written form.

19.2 Number of Counterparts. The Contract is made in **three (3) counterparts** in the Czech or English languages, of which the **Client** will receive **two (2) counterparts** and the **Contractor** will receive **one (1) counterpart**.

19.3 Relationship between the Contract and its annexes. In the event of any discrepancy between the text of this Contract and its Annexes, the text of the Contract will prevail.

19.4 Annexes. The following annexes form an integral part of the Contract:

19.4.1 Annex 1: Technical and functional description of the queue management and passenger flow measuring system

19.4.2 Annex 2: Contact Details

19.4.3 Annex 3: Process and phases of installation of the queue management and passenger flow measuring system

19.4.4 Annex 4: Security requirements to be included in contracts

19.4.5 Annex 5: ICT Technical Standards

In witness of their consent with the text and contents of this Contract, the Parties have affixed their signatures below.

Date: 16.6.2025	Date:
On behalf of the Client:	On behalf of the Contractor:
Signature: _____	Signature: _____
Name: Ing. Jiří Pos	Name: [redacted]
Position: Chairman of the Board Letiště Praha, a. s.	Position: [redacted] Xovis AG
Signature: _____	Signature: _____
Name: Ing. Martin Kučera MBA	Name: [redacted]
Position: Member of the Board Letiště Praha, a. s.	Position: [redacted] Xovis AG

Annex 1 Technical and functional description of the queue management and passenger flow measuring system

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 passport control
FIDS	Flight Information Display System	-
GUI	Graphical User Interface	-
HK	Passport 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 passport control counters.
EU ABC	European Union Nationality – Automated Passport Control	Travellers with EU (and EEA) nationality passing through automated passport control e-gates.
All passports ABC	Third-Country Nationals - Automated Passport Control	Passengers with EU (and EEA) nationality passing through automated passport 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 passport 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 passport 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 passport 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 passport 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) passport 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:
  - the current waiting time
  - the number of persons waiting in an area/queue;
  - the number of active gates/counters at a checkpoint;
  - 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 passport control;
- monitored checkpoints (passport control, security check)
- an overview of SLA violations at security and passport control checkpoints over a specific period of time;
- throughput (process times) for individual lines for security and passport 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 passport 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

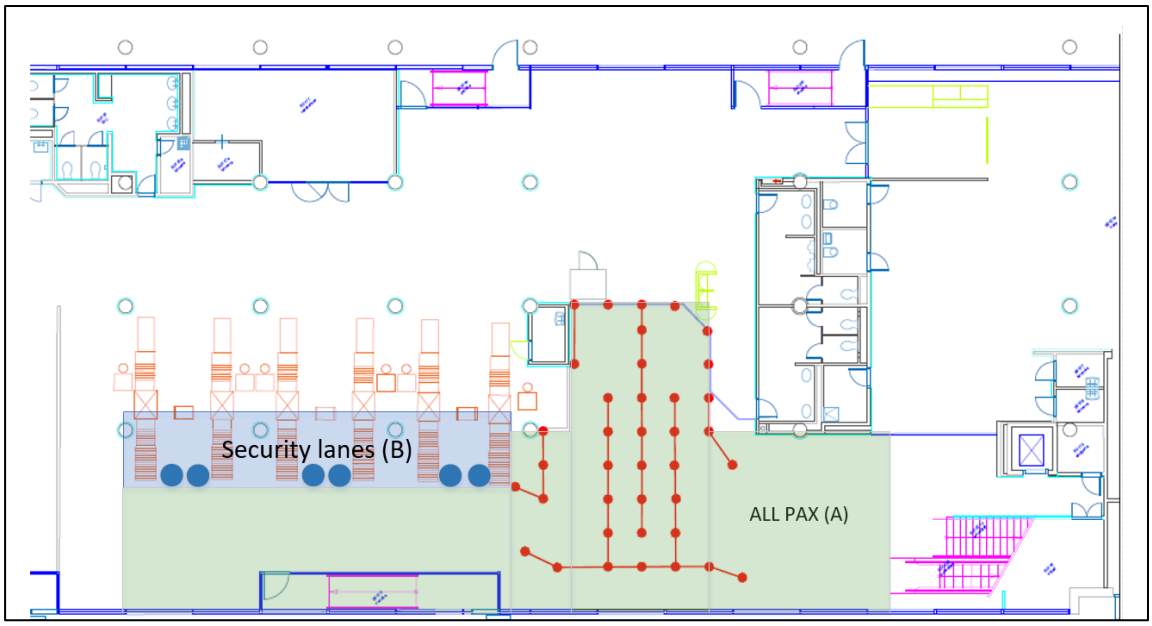
Departure Passport Control

The departure passport 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 passport 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 passport 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

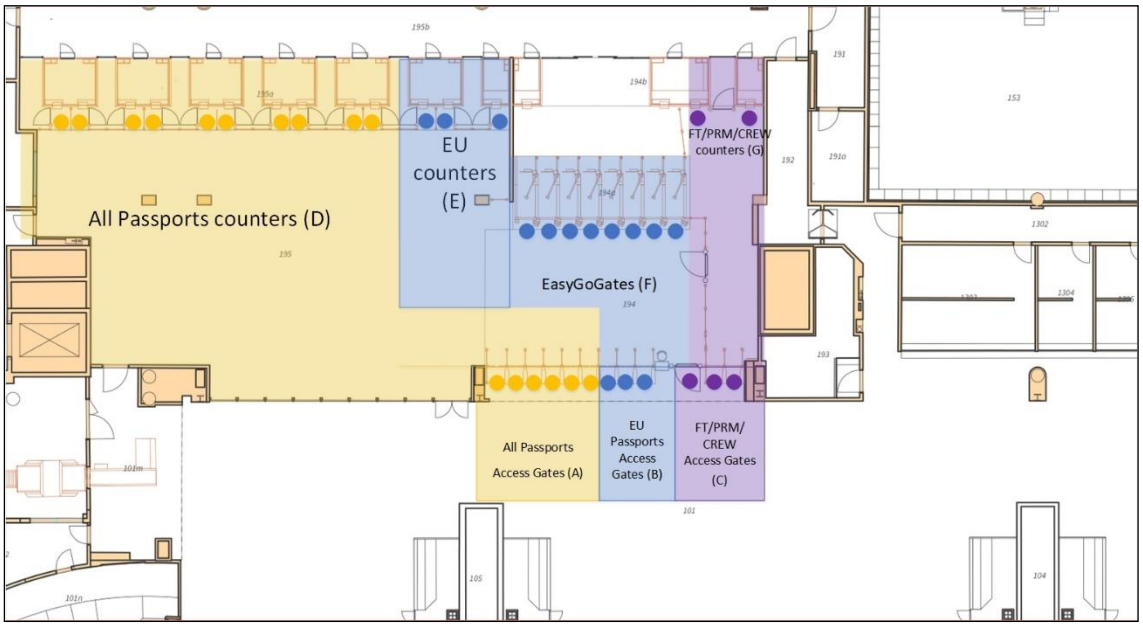


Centralised security check in pier B

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 Passport Control

Arrivals passport 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.

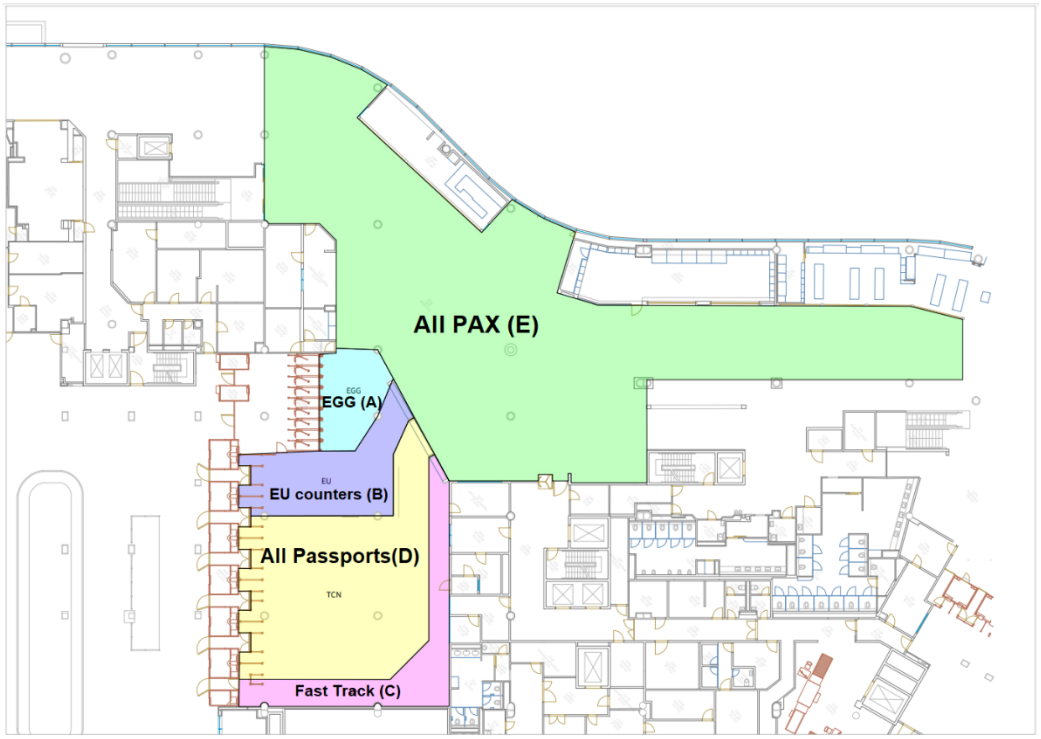
Passenger flows are divided before the passport control point itself as follows:

- passengers who are authorised to use automatic passport 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 passport control area, the LP aims to monitor the corridors leading to this checkpoint, namely the corridors from piers A and B.

Dimensions

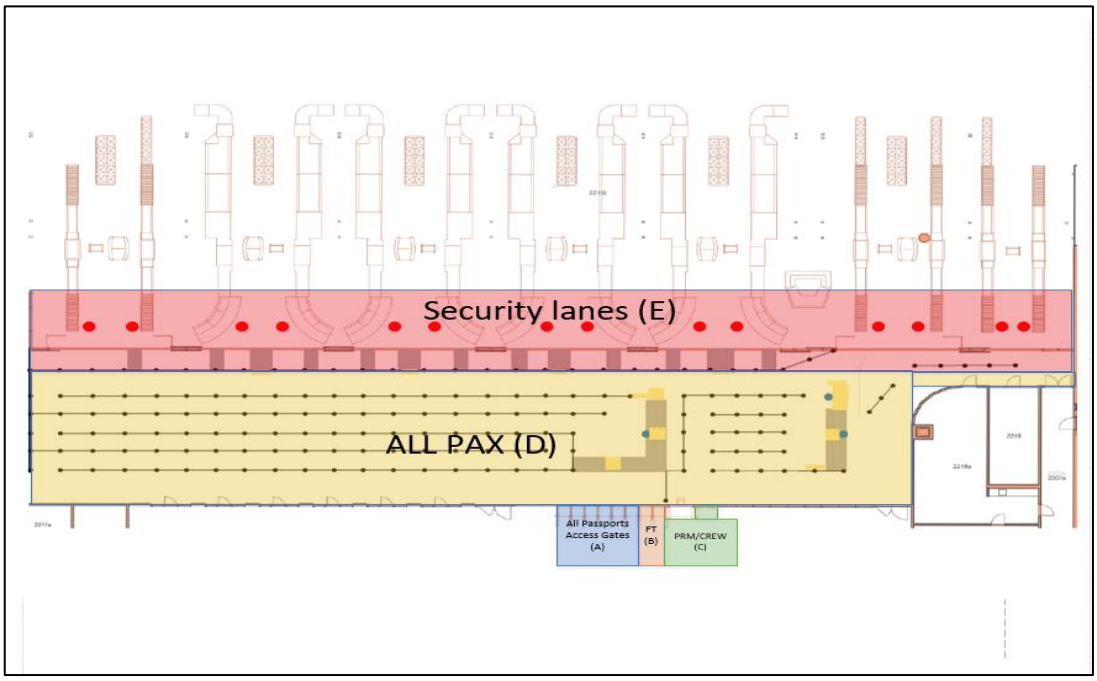
- Area size:
  - A = 77 m^2
  - B = 108 m^2
  - C = 82 m^2
  - D = 492 m^2
  - Ceiling height (A-D): 2.5 – 3.5 m
  - E = 848 m^2
    - Ceiling height = 3.9 m



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 check in pier B (T1)

Phase 2: Departure passport control (T1)

Phase 3: Arrival passport control (T1)

Phase 4: Centralised security check (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 passport 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 passport 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 exports of selected measured and stored data to the Prague Airport 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

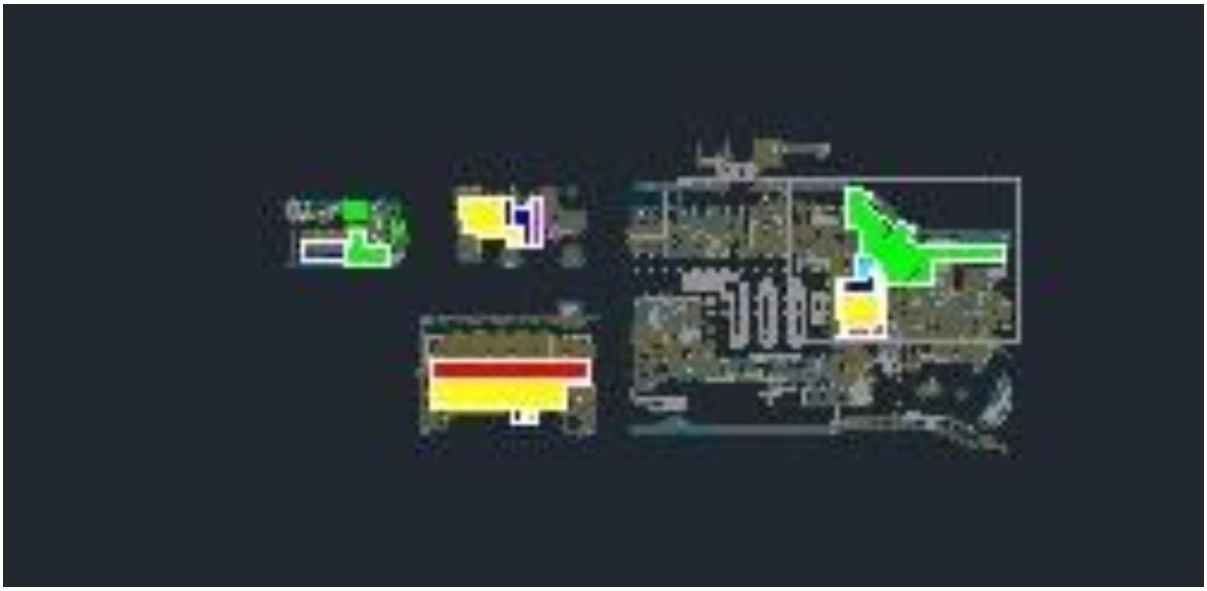
Passenger data

ID PAX	Queue entry time	Queue	Predicted waiting time [min]	Counter / lane	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:



Annex 2: Contact Details

Delivery address.

(a) Client's address for service:

Letiště Praha, a. s.
K Letišti 1019/6, Praha 6, postal code 161 000
Czech Republic

into the hands of: ICT Executive Director

(b) Contractor's address for service:

Xovis AG
Industriestrasse 1, 3052 Zollikofen, Switzerland

Responsible persons:

The responsible representative to represent the **Contractor in contractual matters** related to the performance of this Contract is:

The responsible representative to represent the **Contractor in technical matters** related to the performance of this Contract and in the matter of the Assignment, Tenders and Orders is:

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

The responsible representative to represent the **Client in technical matters** related to the performance of this Contract and in the matter of the Assignment, Tenders and Orders is:

Name	E-mail	Telephone	Mobile

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:

(a) Occupational safety: bozp@prg.aero

(b) Environment: zivotni.prostredi@prg.aero

(c) Fire prevention: technik.po@prg.aero

(d) Complaints: stiznosti@prg.aero

Client's contacts – authorised persons in the matter of handling Defects

Name	E-mail	Telephone	Mobile
[redacted]			
[redacted]			

Escalation contacts on the part of the Client:

Order	Contact	Person	Telephone
[redacted]			

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 Defects. 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	Mobile	Cause of escalation
[redacted]				1st level of escalation in the

Annex 3 – Process and phases of installation of the queue management system

The deployment of the queue management system in Prague Airport locations/phases will be carried out according to the following procedure:

Phase 1 – Terminal 1 Centralised security checkpoint in pier B

Phase 2 – Terminal 1 Departure Passport Control

Phase 3 – Terminal 1 Arrival Passport Control

Phase 4 – Terminal 2 Centralised Security Checkpoint

The Client reserves the right to modify the proposed phasing.

Annex 4 – Security Measures

The purpose of this Annex 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 "SW" or "HW"), or who, in connection with the performance for the Client, access the Client's information system (hereinafter also "LP IS") which is certified in accordance with ISO/IEC 27001:2013 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").

1. GENERAL REQUIREMENTS

The Contractor undertakes to fulfil the following obligations when providing performance for the Client:

a) 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;

b) 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 the "**Contact Person**") within 3 days after the conclusion of the Contract.

c) If personal data is processed in the performance of the subject of the Contract, the Contractor undertakes to ensure that a separate annex is concluded in accordance with the relevant provisions of the GDPR;

d) to 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. SECURITY REQUIREMENTS FOR SW DEVELOPMENT

When providing performance to the Client, the Contractor agrees:

a) Within the time limit set by the Client, or without undue delay, provide the Client with required cooperation to perform security testing during software development or after its handover;

b) To deliver system and operational safety documentation by the handover and acceptance of the SW in a manner specified in the Contract,

c) that the performance includes only those parts that are objectively necessary for ensuring proper the SW operation and/or that are explicitly specified in the Contract (in particular that the SW does not contain any unnecessary components, any programmable samples, unnecessary third-party software, etc.);

d) 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;

e) Any and all confidential information[1] provided to the Contractor 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;

f) 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);

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

[1] Within the meaning of this Annex, confidential information includes, in particular, certificate identification information, passwords, configuration files, system programs, critical libraries, recovery procedures, etc.

h) 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).

i) That if the performance includes SW implementation in the LP's IS production environment, new SW or new SW versions may be installed only subject to migration procedures that have been pre-approved by the Client[2];

3. PHYSICAL PROTECTION AND ENVIRONMENTAL SAFETY

a) 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,

b) 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

In the event that LP's employees have access to external web services, the following requirements must be met:

a) Login information must not be stored in a readable format and must be protected by sufficiently strong encryption means.

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

c) If penetration testing results in critical findings, the Contractor is obliged to immediately inform the LP of these facts and to take additional, effective Remedial Measures.

d) The LP reserves the right to perform penetration testing throughout the term of the Contract.

e) 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:

a) 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.

b) 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.

c) 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 employees with assigned access (physical, logical) to the ICT system must demonstrably consent to the processing of personal data during the evaluation of data on movement and activities performed on the Client's premises (such as monitoring with the Security Incident and Event Monitoring solutions); such consent must have the form of written or digital consent by e-mail unless otherwise agreed by the Parties.

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

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

[2]Migration procedure – a set of steps defining the conversion of data between two or more ICT systems.

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

g) The Contractor undertakes that before connecting an end device, mobile end device or active network element such as network switches, WiFi access points, routers or hubs to the computer network, it will request approval of the connection from the Contact Person on the Client's side

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

i) 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.

j) 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.

k) 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.

l) 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;
   - do not store and/or share company data and information in unauthorised data repositories or media; do not send chain emails.

m) 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 anti-virus protection installed, running and updated;

n) 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

a) 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.

[3] Data and information containing elements of extremism, terrorism, pornography or incitement to intolerance and social prejudices relating to a social group identified on the basis of race, religion or belief, gender, sexual orientation, nationality and ethnicity, or other differences.

b) 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.

6. HANDOVER AND ACCEPTANCE OF PERFORMANCE

a) The Contractor acknowledges that failure to comply with the Safety Requirements, including the requirement to submit complete system and operational documentation, is a Defect preventing acceptance of the subject matter of the Contract (it is a Category A Defect), and the Client is not obliged to accept the performance until the relevant Defect has been removed.
b) The Contractor is liable for ensuring that ICT systems contain the latest security updates (patches) [4].

7. DATA USAGE RIGHTS

a) 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.
b) During their performance of the Contract, the Contractor agrees to dispose of data for the Client only in accordance with the Contract and the relevant legislation, in particular the Cyber Security Act, the Decree and other related legislation.

8. EXCHANGE OF INFORMATION

a) 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.
b) 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.
c) The Contractor undertakes that online transactions carried out via web technologies will be protected by SSL certificates.

9. 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.

10. BUSINESS CONTINUITY MANAGEMENT

a) 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.

[4] Upgrade the software to a higher development version.

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

c) 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.

Annex 5 – 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 (13) (14) AIX	(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
(20) Other applications/systems (21) (22) (23) (24) (25)	(26) UNIX (27) (28) Linux (29) (30) Windows (31) (32) 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	(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

	(53)	
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) (79) MS IIS (80) GlassFish	2.4. and above IIS 10 and above 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

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: