Questions & Answers; Common Use			
Question number	Name of document, section and page number	Question	Answer Eindhoven Airport (EANV)
1	Appendix 2b – Requirements → D17, D18, D19	Could you please confirm that Hardware preventive maintenance could be done by EANV employees? and preventive maintenance that is mentioned in the supplier responsibilities is on the Software/Platform side only?	Preventive maintenance is subject to requirements D17, D18 and D19. There is a typo in requirement D19. Requirement D19 must be: "Any preventive maintenance tasks, with a frequency lower than monthly, shall be performed by Participant's staff."
2	Appendix 2a – Schedule of Requirements – Chapter 2, Section 2 "Teams" (Airport Operations, TS&FM and D&IT availability)	For incidents outside the working hours of local airport engineering teams, does EANV expect the supplier to provide full remote diagnostics independently, or are airport operations personnel available to perform basic hands-and-eyes activities?	In that situation, we expect the Supplier to be fully self-sufficient and able to operate independently. Airport Operations staff may provide best-effort support within their knowledge and availability, but their primary responsibility remains airport operations.
3	Appendix 2b – Requirements – D20	Regarding the following point: "The Participant will perform a full system health check at least once every six months. This health check shall be performed inperson, on-site.", could you please clarify what are the activities expected during this health check? Is this for HW and SW? can the SW health check part be done remotely?	We consider it important to have product expert on-site at least every 6 months to verify the state of local hardware, observe usage of the system and identify any improvements, adjustments or other enhancements. Also, preventive maintenance tasks can be performed during this visit as per requirement D19. Software health checks that can be performed remotely, are permitted to be executed remotely.
4	Annex 9 - Security_Annex, Appendix 2b - Requirements, – Section 4 "Penetration tests, audits, technical risk assessments" (4.1) & requirements E18-E19	Given that many suppliers operate under established certification and audit frameworks (e.g., ISO 27001, ISO 20000, SOC attestations), would EANV agree that existing third-party assurance reports satisfying the intent of Requirement 13.5 are sufficient, and that no additional TPM shall be required?	The reference to Requirement 13.5 is currently unclear, as no such requirement can be identified in the tender documentation. The Participant is requested to clarify which specific requirement is being referred to during the next round of questions. Subject to this clarification, we agree that existing third-party assurance reports may satisfy the intent of the requirement, provided that the Participant can, upon request, provide a valid TPM, a SOC 2 Type II report, or an equivalent ISAE 3000 Type II assurance report covering the relevant scope. ISO 27001 certification alone shall not be considered equivalent to a TPM. Notwithstanding the above, we reserve the right to perform an audit, penetration test, or other security assessment where justified by risk, compliance, operational, or security considerations. Such rights shall remain unaffected by the existence of any certification, assurance report, or TPM.
5	Standard Form- Pricing sheet	In the Customer Pricing Form, the section titled "Fictitious costs – On-premise virtual servers" is highlighted in yellow, which would normally indicate that it should be completed by the bidder. However, the field appears to be a predefined drop-down and cannot be amended by us. Could you please confirm whether this section is intended to be completed by the customer and therefore should be left unchanged by bidders, or whether bidders are expected to provide any input in this field? Additionally, if bidder input is required, could you please clarify whether this field should be completed when the proposed solution is deployed on-premise?	The bidder should input these fields (cell D41 and D54). Please refer to chapter 6 of the Schedule of Requirements for further explanation on how these fictitious costs are defined. You have four options of "resource usage" that lead to a certain fictitious cost level (one-off and per year).
6	Tendering Guide – 5.6 Quality assurance requirements	With reference to SR6 and Requirement E18, our understanding is that SR6 requires the Participant to hold and submit a valid ISO/IEC 27001 certificate but does not expressly require the certification scope to cover the offered CUPPS solution, while E18 separately evaluates whether the certified scope covers the organisational activities relevant to the development, implementation, maintenance and support of CUPPS. Can EANV therefore confirm that SR6 may be satisfied by submitting a valid ISO/IEC 27001 certificate held by an affiliated company within the Participant's corporate group, where the certified ISMS covers central security operations and supporting infrastructure used to support the services provided under the Engagement, even if that certificate does not demonstrate full compliance with the specific scope described in E18?	Correct, SR6 does not expressly scope to the offered CUPPS solution. Requirement E18, which is a High priority requirement (and thus not a knock-out) does. However, the Participant submitting the Tender must itself satisfy SR6. Reliance on an affiliated company is only possible through participation as a Consortium; see section 2.8 of the Tendering Guide.
7	Appendix 2b - Requirements – A2. Workstations and peripherals	With reference to requirement A35, given that CUPPS environments typically operate under controlled security policies, can EANV please clarify the specific troubleshooting, and analysis activities that customer personnel are expected to perform on CUPPS workstations that would require elevated or local administrative permissions?	In our experience, it can be helpful—although it is not mandatory—for EANV staff to have the ability to use a privileged account, e.g. for root cause analysis or to support the Participant's support desk.
8	Appendix 2b - Requirements – C2. Acceptance and go-live	Requirement C13 states that the penetration test will be performed by an independent third party appointed by EANV. Please confirm that EANV will contract and bear the costs of this independent penetration test. Please also confirm that the scope, methodology, rules of engagement and classification of findings will be agreed with the Participant in advance, and that acceptance will not be withheld where a reported Critical or High finding is not attributable to the supplied solution, is a false positive, or is subject to an agreed remediation or mitigation plan.	Yes, EANV will contract the third party and bear the costs. We confirm that the scope, methodology, rules of engagement, and classification of findings will be agreed with the Participant in advance. EANV confirms that acceptance will not be withheld solely on the basis of a Critical or High finding that is demonstrably not attributable to the supplied solution, constitutes a false positive, or is subject to a remediation or mitigation plan that has been reviewed and accepted by EANV. Any remediation activities required to address identified findings are on the account of Participant and cannot be charged to EANV as they contribute to the general quality of the Participant's product.
9	Appendix 2b - Requirements – E1. Cyber Security	With reference to Requirement E11, please confirm that 24/7 monitoring applies to security events generated by the security-relevant components within the Participant's operational control and does not constitute a guarantee that every potential incident or breach will be detected.	We understand that we cannot expect 100% detection of (potential) security incidents. The Participant's detection capabilities must be modern and well designed, and detected events must be acted upon appropriately.
10	Appendix 2b - Requirements – E1. Cyber Security	With reference to Requirement E12, please clarify the expected minimum frequency and scope of automated vulnerability scanning, including whether the requirement applies to workstations, operating systems, servers, application components and third-party software. Please also confirm that scanning of components or infrastructure managed by EANV will remain under EANV's responsibility.	We expect automated vulnerability scanning to be performed at least once per week, but preferably on a daily basis. The scope of the scanning shall include all systems, infrastructure, operating systems, servers, application components, workstations, third-party software, and any other assets managed by the Participant that are relevant to the delivery or operation of the services provided to EANV. We further confirm that the scanning and management of infrastructure and components that are managed by EANV remain the responsibility of EANV. The Participant is responsible for vulnerability scanning and remediation activities within its own environment and for all assets under its management that support the services delivered to EANV, including but not limited to CUPPS workstations.
11	Appendix 2b - Requirements – E1. Cyber Security	With reference to Requirement E15, where direct integration with EANV's SIEM is not technically supported by the standard solution, would EANV accept an alternative arrangement under which relevant security events and alerts are monitored by the Participant and communicated to EANV through the agreed incident notification and security reporting channels?	This requirement requests SIEM integration. If that is not possible, the requirement must be responded to accordingly.
12	Appendix 2b - Requirements – E1. Cyber Security	With reference to Requirement E16, please confirm that the 80% target applies only to components for which an applicable CIS Benchmark exists, using an agreed benchmark version and profile, and that the score will be calculated against applicable controls only, excluding controls that are not technically applicable or that would adversely affect the supported operation of the solution.	Components for which no CIS Benchmark exists may only be excluded where no equivalent hardening standard, vendor hardening guidance, or alternative security baseline is available. Where such guidance exists, it shall be applied and considered as part of the security baseline. EANV acknowledges that certain CIS controls may not be implementable where doing so would negatively impact the supported operation or functionality of the solution. In such cases, the Participant shall document the rationale for the exception and any compensating security measures. The operational stability and functionality of the solution remain the primary consideration. However, exceptions to CIS controls do not automatically exempt the Participant from meeting the 80% compliance target. If justified exceptions result in a compliance score below 80%, the Participant shall discuss this with EANV. Any deviation from the minimum compliance requirement shall be subject to EANV review and approval. In addition, the Participant shall review and reassess its hardening baseline at least once every year against the latest available version of the applicable CIS Benchmark, vendor hardening guidance or alternative security baseline. Where relevant improvements or new security measures are identified, these shall be evaluated and implemented in a timely manner, taking into account the operational stability and functionality of the solution.
13	Appendix 2b - Requirements – E1. Cyber Security	With reference to Requirement E19, please confirm what forms of equivalent independent third-party assurance EANV would accept where the Participant does not hold a SOC 2 Type II report covering the specific organisational scope described in the requirement.	An ISAE 3000 Type II report, which is generally recognized as the European equivalent of a SOC 2 Type II report, will also be accepted provided that it covers the relevant organisational scope and includes an assessment of the design and operating effectiveness of the security controls over a defined period.
14	Annex 2 - General Purchase C – 20. Security	Please confirm that the obligation under Article 20.2 to report suspected Security Incidents will be aligned with Clause 12.1 of the Security Annex and will apply when the Participant confirms a Security Incident affecting EANV Data, assets, systems or Services, rather than to every event or unconfirmed suspicion being investigated.	Yes, clause 12.1 of the Security Annex is limited to what's described in Article 20.2 of the General Purchase Conditions. This includes any shared components of Participant's infrastructure, e.g. a compromised mailbox that may contain EANV Data, or a lost laptop that may contain log files of EANV.
15	Annex 9 - Security Annex – Chapter 1: About this document	The Security Annex states that, following formal contract formation, risks related to the system or service will be identified through a Business Impact Analysis and that the resulting cyber security requirements will be implemented by the Contractor. Please confirm that the Business Impact Analysis will be owned and led by EANV, with the Participant's reasonable cooperation. Please also confirm that any additional requirements resulting from the Business Impact Analysis will be subject to mutual assessment and agreement regarding applicability, technical feasibility, responsibilities, costs and implementation timelines.	Yes, the Business Impact Analysis (BIA) will be owned and led by EANV. Additional requirements will be subject to mutual assessment. EANV expects that most resulting requirements will already be met where the Participant applies a mature cybersecurity framework.

16	Annex 9 - Security Annex – Penetration tests, audits, technical risk assessments	Please confirm that any penetration test, security scan, technical risk assessment or audit under Clause 4.1 will be limited to the systems and services processing EANV Data and will be subject to prior agreement with the Participant regarding scope, methodology, timing and rules of engagement. Such activities should not affect production availability, shared environments, other customers or third-party systems. Please also confirm that findings and remediation timelines will be reviewed and agreed by both Parties.	We confirm that the scope, methodology, rules of engagement, and classification of findings will be agreed with the Participant in advance. However, the scope of such activities shall not be limited solely to systems and services processing EANV Data. It shall also include systems, services, and supporting infrastructure that is relevant to the delivery or operation of the services provided to us. We further confirm that findings and remediation timelines will be reviewed and discussed by both Parties. Any agreed remediation timelines shall take into account the severity of the findings, the associated risks, and the operational requirements of the service.
17	Annex 9 - Security Annex – Passwords / Multi-factor authentication	With reference to Clauses 6.1 to 7.2 of the Security Annex and Requirement E5 of Appendix 2b, please confirm that the password requirements apply only to accounts managed by the Participant and do not apply to end-user accounts authenticated through an EANV or handler-managed Identity Provider. Please also confirm that EANV and the relevant handlers remain responsible for the identity lifecycle, authentication policies and corporate credentials of their federated users.	We agree and confirm.
18	Annex 9 - Security Annex – Security incidents	With reference to Clauses 12.1 to 12.3 of the Security Annex, please confirm that the notification obligation applies to confirmed Security Incidents affecting EANV information, systems or the Services, rather than to every event or unconfirmed suspicion under investigation. Please also confirm that the notification period starts when the Participant confirms the incident and its impact on EANV, and that the initial notification may contain the information reasonably available at that time, with further information provided as the investigation progresses. In addition, please remove the word "exclusively", as the Participant may also be required to notify competent authorities, insurers, advisers, other affected customers or third parties in accordance with applicable legal, regulatory or contractual obligations.	Yes, clause 12.1 of the Security Annex is limited to what's described in Article 20.2 of the General Purchase Conditions. The notification period starts when Participant became aware of the (presumed) incident, not when it confirms it (as it is rather vague what confirming means in this context). We fully acknowledge that an initial notification may contain very limited information when an incident is still under investigation. We believe transparency and early notification are important to establish partnership and to enable EANV to support Participant in any way resolving the incident. We will remove the word 'exclusively'. Article 12.1 of the Security Annex will be amended as follows: 12.1Whenever the contractor identifies any actual or presumed security incidents relating to EANV Data, assets, systems or services to EANV, the contractor must report them to EANV immediately, but in any event within 24 hours after the contractor became aware of them.
19	Tendering Guide – 5.1 SR1 Corporate guarantee	Could you please clarify whether the requirement for a parent company guarantee is mandatory in all cases? In particular, would you please consider accepting alternative forms of financial security (such as demonstrable financial stability of the supplier, combined with a bank guarantee for performance) as an equivalent to a parent company guarantee, and as per standard practice?	We have decided to drop the requirement for a corporate guarantee. SR1 will not be applicable.
20	Appendix 1. Agreement – 5.2 Deliveries	Could you please confirm that: (1) delivery penalties apply only where the delay is caused solely and directly by the Supplier; and (2) such penalties are the sole and exclusive remedy for that delay? Additionally, and to preserve balance and cash flow certainty for both parties, we would kindly ask the Customer to consider removing the unilateral right of set-off. The Supplier confirms that any penalties or service credits accrued would instead be credited in the Supplier's next invoice to the Customer.	EANV does not agree. A penalty may be imposed where the Supplier fails to meet a contractual deadline and that failure is attributable to the Supplier under the Agreement or applicable law. The contractual penalty is not intended to replace compensation for damages and is without prejudice to EANV's right to claim full compensation for the actual damages suffered. Contractual penalties are therefore not the sole and exclusive remedy, as delay may cause damage exceeding the amount of the penalty and may affect the operational continuity of the airport. EANV's right of set-off is retained. The Tender Documents will not be amended.
21	Appendix 1. Agreement Annex 8 - Data Processing Agreement – Appendix 1 . 6.5 Fees and payment Appendix 1. Annex 11 (Exit Plan) 11. Verification and audit Annex 8. 6. Audit requirements	Could you please confirm that, in line with standard practice, any audit must be notified to the Supplier in writing at least thirty (30) days in advance, that audits may be conducted no more than once (1) per year, and that the Supplier shall grant access solely to the records and information relevant to such audit. Further, please confirm that, where an audit identifies non performance, the Supplier will bear the costs of remedying such non performance, but not the full costs of the audit itself.	EANV does not accept a fixed notice period or a general restriction limiting audits to one audit per calendar year. Such limitations would be inappropriate in situations requiring an urgent or additional audit, including incidents, regulatory requests, material non-compliance, or exit and transition verification. EANV will exercise its audit rights reasonably. Audits will be announced in writing within a reasonable timeframe, limited to the scope of the Agreement and the purpose of the audit, conducted subject to appropriate confidentiality obligations, and carried out in a manner that minimises disruption to the Supplier's business operations. Access shall be limited to information reasonably necessary for the audit. In this respect, EANV refers to Article 13 of the General Purchase Conditions. In accordance with Article 13.1, audits initiated by EANV are conducted at EANV's own expense. The General Purchase Conditions do not provide for a general transfer of audit costs to the Supplier. However, the Supplier remains fully responsible for the proper performance of its obligations and shall bear the costs associated with remedying any non-performance, in accordance with the Agreement and applicable provisions. Furthermore, as set out in Article 13.5, any TPM reports requested by EANV shall be provided by the Supplier at its own expense. The provisions remain unchanged.
22	Appendix 1. Agreement – 6.7 Fees and payment	Could the Customer please consider amending the indexation mechanism so that the Supplier may index the rates annually from Year 2 of the Agreement, rather than only after the first renewal, subject to the same requirements? This reflects standard practice and inflationary cost increases over the initial term.	Accepted. Article 6.7 of the Agreement will be amended as follows: Supplier may index the rates as set out in Annex 5 or in the Agreement annually, but only after the first year of the term of this agreement, with a maximum of the percentage of the index for Business Services, 2015=100, turnover development index compared to a year earlier (Zakelijke dienstverlening (M-N) 2015=100, index omzetontwikkeling t.o.v. een jaar eerder)], published in the second quarter of the previous year by Statistics Netherlands (Centraal Bureau voor de Statistiek), in any event with a maximum of 5%. The Supplier must inform EANV ultimately on 1 September whether it wishes to index the rates for the coming year and with what percentage. If the Supplier fails to do so, the Supplier is not entitled to index the rates for the coming year.
23	Appendix 1. Agreement – 8.3 Reports and KPI	Could the Customer please confirm and amend as follows: (1) penalties apply only where the failure is caused solely and directly by the Supplier, and only after a reasonable remedy period following written notice; (2) penalties are the sole and exclusive remedy for the relevant failure; and (3) the unilateral right of set-off is removed, any penalties or service credits instead being credited in the Supplier's next invoice to the Customer?	EANV does not agree. A penalty may be imposed where the relevant failure is attributable to the Supplier under the Agreement or applicable law. Given the operational importance of the service levels and KPIs, no general notice or remedy period applies before a penalty becomes due. Notwithstanding the foregoing, where EANV reasonably considers this appropriate in the circumstances, EANV may, at its sole discretion, first provide the Supplier with written notice of the relevant failure and grant a reasonable period to remedy such failure before imposing a penalty. Any such remedy period shall be determined by EANV, taking into account the nature and urgency of the failure. Penalties are not the sole and exclusive remedy, and EANV's right of set-off is retained.
24	Appendix 1. Agreement – 5.2 Deliveries 8.3 Reports and KPI	Could the Customer please confirm that all penalties under the Agreement are subject to a single aggregate cap? In line with standard practice, the Supplier proposes an aggregate cap of 10% of the annual contract value.	EANV partially accepts the request. Article 8.3 of the Agreement will be replaced by: If Supplier fails to meet any service level, KPI, availability requirement, response time, resolution time, reporting ob-ligation or other service performance requirement set out in Annex 1, Annex 4 or Annex 7, EANV shall be entitled, but not obligated, to impose a penalty calculated on the monthly recurring fees for the affected Deliveries. The penalty shall be 5% for the first calendar month in which such failure occurs, 10% for the second consecutive calendar month in which the same or a substantially similar failure occurs, and 15% for the third and each subsequent consecutive calendar month in which the same or a substantially similar failure occurs. Notwithstanding any other provision of this Agreement, the aggregate amount of contractual penalties that may be imposed on the Supplier during any contract year shall not exceed 15% of the annual contract value. Examples of SLA failures include, without limitation, failure to meet agreed availability percentages, response times, resolution times, incident handling requirements, maintenance windows, reporting deadlines, release procedures, or agreed service continuity obligations. The penalty is payable without any notice of default being required and without prejudice to EANV's right to claim performance, damages, termination, rescission or any other rights and remedies available under the Agreement or applicable law. EANV may set off any penalty owed by Supplier against amounts payable to Supplier.
25	Appendix 1. Agreement – 11.1 Exit Annex 11 - Exit Plan	Could you please confirm that any exit assistance will be provided at mutually agreed fees and for a mutually agreed duration?	Yes, this is already covered in section 9 of Annex 11 (Exit-Plan).
26	Appendix 1. Agreement – 11.3 Exit	Could you please clarify that the provision applies only to failures directly and solely attributable to the Supplier, following a reasonable opportunity to remedy (no less than 30-day remedy period)? Could the Customer also confirm that any related costs must be reasonable, properly incurred, and supported by documentary evidence?	Article 11.3 applies where the Supplier fails to comply with the Exit Plan and that failure is attributable to the Supplier under the Agreement or applicable law. EANV does not agree to a fixed 30-day remedy period, as the appropriate period depends on the nature and urgency of the deficiency and the need to safeguard continuity, security and data protection. Costs passed on to the Supplier must be reasonable, demonstrably incurred and causally related to the Supplier's failure.

27	Appendix 1. Agreement – 12.1 Deviations	We note the proposed liability cap of EUR 500,000 per event and EUR 1,500,000 per calendar year. Given the value of the Agreement, the annual cap is substantial, and, as it resets, the aggregate exposure over the whole term of the Agreement would be a multiple of the fees payable. This is significantly above both the contract value and market practice, under which liability is typically aligned to the fees paid. Could the Customer please consider limiting the Supplier's aggregate liability for all claims under the Agreement to the total fees paid or payable to the Supplier over the contract term?	EANV does not share the view that market practice generally requires liability to be capped at the fees paid or payable under the Agreement. The appropriate level of liability depends on the nature of the services and the risks involved. Nevertheless, EANV is prepared to reduce the liability cap to EUR 500.000 per event and EUR 1.000.000 per calendar year. Article 12 of the Agreement will be amended accordingly: "Pursuant to Article 18.2, the Parties agree that the Supplier's liability as referred to in Article 18.1 of the General Purchase Conditions is limited to an amount of EUR 500.000 per event, with a maximum of EUR 1.000.000 per calendar year." Also, Suitability Requirement SR2 will be amended accordingly, as per section 5.2 of the Tendering Guide: 5.2.SR2 Corporate and professional liability insurance The Participant declares •that it has sufficient liability insurance under a corporate and professional liability insurance policy. This insur-ance provides at least €500.000,00 of cover per loss event up and at least €1.000.000,00 per year, and •that the insurance will be maintained during the entire term of the contract. The Participant declares that it will provide the insurance policy/insurance certificate or the declaration of the insurance company within 10 calendar days of a request to that effect.
28	Annex 3a - Special Provisions - Hardware – 3.1 Transfer of ownership	Could you please confirm that title to the hardware shall pass to the Customer at the later of (i) delivery of the hardware, and (ii) receipt by Supplier of the applicable hardware payment?	EANV confirms that the title to the Hardware shall pass to EANV at the later of (i) Delivery of the Hardware, and (ii) receipt by the Supplier of the corresponding payment for that Hardware.
29	Annex 3a - Special Provisions - Hardware – 7. Right of use	The Special Provisions grant a perpetual, worldwide, irrevocable and sub-licensable right of use. Could the Customer please clarify the intended scope and purpose of this right, particularly where the Agreement operates as a pure hardware purchase model? Could the Customer please clarify the meaning of "System Software"? Does this refer to third-party software embedded in or supplied with the hardware, or to the Supplier's own software provided under the Agreement?	System Software is defined as follows: "The System Software described in the Agreement that the Parties use (or must use) in combination with the Hardware, including the accompanying Documentation. System Software also includes other (auxiliary) software made available by Supplier." It indeed typically refers to (third-party) software embedded in a piece of hardware, such as firmware. Our intended scope and purpose for this project is solely the operation of the CUPPS platform. Also, EANV may opt to reuse the Hardware in the future after termination of this agreement.
30	Annex 3d - Special Provisions - Software – 3.1 Right of Use	We note that the Special Provisions provide for a perpetual, worldwide and irrevocable Right of Use. As the Software is a Supplier-owned, standard cloud-based solution provided on a subscription basis, could the Customer please confirm that the right to use the Software is limited to the term of the Agreement, on a non-exclusive, non-transferable basis and only for the purposes of this Agreement? Could the Customer please amend the clause accordingly?	A cloud-based system is considered SaaS and explicitly excluded from the definition of Software. However we agree that for CUPPS platforms licensing is typically limited to the term of the Agreement. Therefore we will add the following to article 12 of the main Agreement: Article 3.1 of the Special Provisions Software shall be replaced by the following Article: The Supplier grants EANV a Right of Use to the Software limited to the term of the Agreement in accordance with the Agreement, the General Provisions and the Special Provisions Software.
31	Annex 3d - Special Provisions - Software – 3.3 Right of Use	Could the Customer confirm the Right of Use is non-transferable, and that any transfer or assignment requires the Supplier's prior written consent, which the Supplier may reasonably withhold (including on grounds of compliance with the Right of Use conditions or protection of its intellectual property)?	We confirm that the license is non-exclusive and confirm that the Supplier may withhold. Therefore we will add the following to article 12 of the main Agreement: Article 3.3 shall be replaced by the following Article: The Right of Use is non-exclusive and only transferable to third parties with the consent of the Supplier.
32	Annex 3d - Special Provisions - Software – 3.4 Right of Use	Could the Customer clarify that the reference to location/place means "within the airport"?	We may access the CUPPS platform on a device, e.g. a corporate laptop, while working from home.
33	Annex 3d - Special Provisions - Software – 3.5 Right of Use	Could you please confirm that, for Supplier-owned, standard cloud-based software provided on a subscription basis, the Right of Use shall be limited to access and use of the subscribed service during the Agreement term and shall not include perpetual or unrestricted use, reproduction, hot-standby, or testing/development rights? Could the Customer please amend clause 3.5 accordingly?	If your solution is cloud-based, it is considered as SaaS. The Special Provisions Software do not apply to SaaS. Please refer to the Special Provisions SaaS.
34	Annex 3d - Special Provisions - Software – 3.6 and 3.7 Right of Use	Again, the Software is a Supplier-owned, standard cloud-based solution provided on a subscription basis. Could the Customer please confirm that Clauses 3.6 and 3.7 do not apply to such Software, as access, updates and applicable maintenance are governed by the subscription terms for the duration of the Agreement?	If your solution is cloud-based, it is considered as SaaS. The Special Provisions Software do not apply to SaaS. Please refer to the Special Provisions SaaS.
35	Annex 3d - Special Provisions - Software – 10 Escrow	The solution provided under this Agreement is a standard, mature offering and is not customized or developed specifically for Customer. It is delivered to multiple customers on an identical basis and supported by established business continuity, maintenance, and support arrangements. Given that access to source code without ongoing maintenance would not be operationally usable or provide meaningful risk mitigation, could Customer please confirm that the source code escrow requirement can be removed in its entirety from the Agreement?	Agreed. Escrow is not appropriate for this Agreement. The following will be added to Article 12 of the Agreement: Article 10 shall not be applicable.
36	Annex 3d - Special Provisions - Software – 12.1 (d) Content Maintenance	Could the Customer please confirm that any request to adapt the Software is subject to the Supplier's prior written agreement and reasonable discretion, and that the Supplier is not obliged to implement requested changes? Any agreed adaptation would be subject to a mutually agreed scope, timeline and commercial arrangement.	Yes, we confirm unless it concerns cyber security risks, compliance to industry standards or any other critical requirement as described in this procurement.
37	Annex 3c - Special Provisions - SaaS – 3.1 Right of Use	As the solution is a standard SaaS service provided on a subscription basis for the term of the Agreement, could the Customer please confirm that the Right of Use is limited to the subscribed SaaS, documented functionalities, users and scope agreed under the Agreement, and does not include undocumented functionalities, testing/development rights, or unrestricted third-party use (Article 3.2)? Could the Customer also clarify the intended purpose of sub-licensing to Affiliates?	Yes we confirm, except for testing/development rights. We may want to integrate software with your SaaS (e.g. consuming an API), or perform testing, which we should be permitted to do so. Currently, EANV does not have any affiliate for which a CUPPS platform could be of use. The following will be added to Article 12 of the Agreement: Article 3.1 shall be replaced by: The Supplier grants EANV for the duration of the Agreement a worldwide, non-exclusive Right of Use in accordance with the Agreement, the General Provisions and the Special Provisions SaaS.
38	Annex 3c - Special Provisions - SaaS – 7 Escrow	The solution provided under this Agreement is a standard, mature offering and is not customized or developed specifically for Customer. It is delivered to multiple customers on an identical basis and supported by established business continuity, maintenance, and support arrangements. Given that access to source code without ongoing maintenance would not be operationally usable or provide meaningful risk mitigation, could Customer please confirm that the source code escrow requirement can be removed in its entirety from the Agreement?	Agreed. Escrow is not appropriate for this Agreement. The following will be added to Article 12 of the Agreement: Special Provisions SaaS: Article 7 shall not be applicable.
39	General Purchase Conditions – 5.4 Payment terms	Could you please confirm that, prior to the Customer suspending payment, Acceptance must not be unreasonably withheld, and that the Customer will notify the Supplier of any alleged non-compliance, granting the Supplier a thirty (30) day remedy period? Please also confirm that, in any event, once such non-compliance has been remedied, the Customer will comply with its payment obligations.	EANV considers that Article 5.4 already forms part of a balanced contractual framework, in which termination for breach (including notice and cure) is addressed separately in Article 16. Introducing a fixed notice and cure period as a precondition for suspension of payment would unduly limit EANV's contractual flexibility. Therefore, the proposed amendment is not adopted. For the avoidance of doubt, EANV will exercise its contractual rights reasonably and proportionately. Acceptance will not be withheld arbitrarily where the Deliverables comply with the contractual requirements. In the event of identified non-compliance, EANV will, where appropriate in the circumstances, notify the Supplier and provide an opportunity to remedy the issue. Once the relevant non-compliance has been remedied and the applicable contractual requirements for acceptance and invoicing have been satisfied, EANV will comply with its payment obligations in accordance with the Agreement.
40	General Purchase Conditions – 5.6 Payment terms	To preserve balance and cash flow certainty for both parties, we would kindly ask Customer to consider removing the unilateral right of set-off. The Supplier confirms that any penalties or service credits accrued would instead be credited in the Supplier's next invoice to the Customer.	EANV does not accept the proposed amendment.
41	General Purchase Conditions – 5.7 Payment terms	Given that limitation periods may be subject to mandatory statutory provisions under the applicable law, could the Customer please confirm that the 2-year limitation period for Supplier claims applies only to the extent permitted by such applicable law and does not replace or override any longer mandatory statutory limitation periods?	Article 5.7 of the General Purchase Conditions is a contractual limitation period and applies to the extent permitted under applicable law. Any mandatory statutory provision that cannot validly be deviated from will prevail. No amendment is required. Article 5.7 remains unchanged.
42	General Purchase Conditions – 6.4 Acces SNBV	Could the Customer please confirm that the Supplier's responsibility for related costs is limited solely to reasonable and standard costs required for mandatory security screenings by applicable laws or regulations?	Yes, that's confirmed. As described in Chapter 3 of the Schedule of Requirements (Appendix 2a), no security screening is required during the airport closure period.
43	General Purchase Conditions – 10.4 Acceptance	Could you please consider providing that, where no Acceptance Test is agreed, the Delivered goods shall be deemed accepted if the Customer does not notify Supplier of any material non-conformity within two (2) weeks of Delivery? For clarity, use of the goods shall also constitute acceptance.	EANV considers that article 10.4 already covers the described scenario sufficiently. The provisions remain unchanged.

44	General Purchase Conditions – 13 Audit and TPM 24.7 Integrity	Could Customer confirm that audits and inspections during the contract term will: (i) be limited to once (1) per year; (ii) be notified at least thirty (30) working days in advance; (iii) be limited in scope to the contracted Service; (iv) be conducted in a manner that does not disrupt production systems, data, or service availability; and (v) be subject to confidentiality obligations?	EANV does not accept a fixed notice period or a general restriction limiting audits to one audit per calendar year. Such limitations would be inappropriate in situations requiring an urgent or additional audit, including incidents, regulatory requests, material non-compliance, or exit and transition verification. EANV will exercise its audit rights reasonably. Audits will be announced in writing within a reasonable timeframe, limited to the scope of the Agreement and the purpose of the audit, conducted subject to appropriate confidentiality obligations, and carried out in a manner that minimises disruption to the Supplier's business operations. Access shall be limited to information reasonably necessary for the audit. In this respect, EANV refers to Article 13 of the General Purchase Conditions. The provisions remain unchanged.
45	General Purchase Conditions – 14.4 Changes in scope	Given that the Agreement concerns a long-term arrangement involving supplier investments, can Customer please confirm that termination under Article 14.4 applies only in the case of material scope changes, and, in such event, the Supplier would be entitled to payment for services performed, committed costs and other non-recoverable investments up to the effective termination date?	Article 14.4 remains unchanged. In the situation described, where no agreement can be reached on the consequences of a change in scope, EANV is entitled to terminate the Agreement by notice. In accordance with Article 14.4, termination under this provision shall not entitle either Party to compensation for any damage. For the sake of completeness, EANV notes that payment shall be made on a pro rata basis for Deliveries performed up to the effective date of termination. No additional compensation (including compensation for committed costs or non-recoverable investments) shall be payable.
46	General Purchase Conditions – 16.1 Suspension and termination	Could you please clarify the rationale for including a termination for convenience provision in this contract? Considering the investment and long-term commitment from the Supplier, would it be possible to limit termination for cause only?	Article 16.1 of the General Purchase Conditions shall not apply. Article 3.1 of the Agreement shall apply instead. For clarity, the following will be added to Article 12.1 of the Agreement: Article 16.1 shall not apply.
47	General Purchase Conditions – 16.3 Supension and termination	Could you please confirm that such "reasonable period of time" to remedy a defect will be, as per the standard, no less than thirty (30) days?	Article 16.3 remains unchanged. A reasonable remedy period depends on the nature, severity and operational impact of the breach. A fixed minimum period of 30 days would be inappropriate for urgent defects, security incidents or failures affecting airport operations. EANV will determine a reasonable period in the circumstances, taking into account the Supplier's ability to remedy and EANV's legitimate interests.
48	General Purchase Conditions – 17.3 Force Majeure	Could Customer please confirm that (i) this right applies only to extraordinary events outside Customer's reasonable control, (ii) any suspension shall be limited to the services directly affected, and (iii) during any suspension the Supplier shall remain entitled to payment for services performed and unavoidable or committed costs incurred?	Article 17.3 intentionally grants EANV the flexibility to suspend the Agreement in the event of a crisis or other exceptional circumstance that has a significant impact on its operations and results in a temporary absence of need for the Supplier's services. The confirmations requested by the Supplier would materially alter the allocation of rights and risks set out in the General Purchase Conditions. In particular, the Conditions do not limit EANV's right of suspension to force majeure situations, nor do they provide for continued payment or compensation during a suspension period. For these reasons, EANV cannot provide the requested confirmations. Article 17.3 remains unchanged.
49	General Purchase Conditions – 18.3 Liability and insurance	With respect to the definition of "direct damages", can Customer consider replacing the wording "shall include" with "may include", and confirm that the items listed are illustrative examples only, to be assessed on a case-by-case basis taking into account the specific circumstances, causation and reasonableness of the alleged damage, rather than applying automatically or exhaustively in all cases?	EANV does not agree to replace "shall include" with "may include". Article 18.3 remains unchanged, as the current wording is sufficiently clear. Article 18.3 is intended to provide clarity regarding the categories of loss that qualify as direct damages under the Agreement. The wording"shall include at least, but not exclusively" expressly means that the listed items are deemed examples of direct damages and that the list is non-exhaustive. At the same time, the provision does not imply that every listed item automatically qualifies for compensation in every case. Any claim for damages remains subject to the applicable legal requirements, including the existence of a causal link between the breach and the alleged damage, as well as the substantiation of the costs or losses claimed. The assessment of a claim will therefore always depend on the specific facts and circumstances of the case.
50	General Purchase Conditions – 18.5 Liability and insurance	Could Customer please consider including letter c), confidentiality, under the standard liability cap, as set out in the Agreement (12.1 Deviations)?	EANV does not agree to the proposed amendment. We consider confidentiality as a fundamental part of partnership. Therefore, Article 18.5 remains unchanged.
51	General Purchase Conditions – 18.6 & 18.9 Liability and insurance	Could Customer please confirm that such indemnification applies when (i) the claim is directly and solely attributable to the Supplier; (ii) when awarded by a final decision of the competent court; and (iii) subject to the liability cap as set out in the Agreement (12.1 Deviations)?	EANV confirms that the indemnification obligation applies where the relevant claim is directly attributable to the Supplier's acts or omissions. With regard to (ii), Article 18 of the General Purchase Conditions already provides an appropriate allocation of risk and does not require a final court decision before the indemnification obligation may arise. With respect to (iii), EANV agrees that the indemnification obligations are subject to the financial liability caps set out in Article 12 of the Agreement. Article 18.9 shall be replaced by the following: "The indemnification obligations set out in this Agreement, including those under Article 18.6, shall be subject to the financial liability caps set out in Article 12 of the Agreement."
52	General Purchase Conditions – 18.7 Liability and insurance	Could you please confirm that, in line with standard practice, any inspection of the Supplier's insurance shall be notified to the Supplier in writing at least thirty (30) days in advance, and that such inspection shall be satisfied by the Supplier providing copies of the relevant and valid insurance certificates?	EANV does not agree to a mandatory notice period of 30 days. Upon request, the Supplier must provide evidence of adequate and current insurance within a reasonable period specified by EANV. In principle, valid insurance certificates and proof of premium payment will suffice, provided they contain sufficient information to verify compliance. EANV reserves the right to request relevant policy terms or further evidence where reasonably necessary.
53	General Purchase Conditions – 20. Security	Please could Customer confirm that the obligation under Article 20.2 to report suspected Security Incidents will be aligned with Clause 12.1 of the Security Annex and will apply when the Supplier confirms a Security Incident affecting EANV Data, assets, systems or Services, rather than to every event or unconfirmed suspicion being investigated?	See answer to question 14.
54	Annex 8 - Data Processing Agreement – 10.1 Information requirements and incident management	Could you please consider amending Clause 10.1 to provide that Supplier shall notify Customer promptly, and in any event within 72 hours of becoming aware of and confirming the relevant incident?	Article 10.1 of the Data Processing Agreement remains unchanged. The notification period of 24 hours is necessary to enable EANV, in its capacity as controller, to comply with its obligations under applicable data protection laws, including the timely assessment of incidents and, where required, notification to the relevant supervisory authority and/or affected data subjects. The obligation relates solely to the initial notification upon becoming aware of an incident and does not require the Data Processor to have completed a full investigation within that timeframe. The Data Processing Agreement already provides that the Data Processor shall cooperate with EANV and supply additional information as it becomes available. Accordingly, EANV considers the current provision reasonable, proportionate, and necessary to comply with the GDPR.
55	Annex 8 - Data Processing Agreement – 12. Liability and indemnity	Could you please confirm that any such failure must be directly and solely attributable to the relevant party, and that its liability shall be limited to direct losses and remain subject to the liability cap set out in the Agreement (12.1 Deviations)?	Article 12.1 of the Data Processing Agreement will be amended to clarify that liability is limited to direct losses directly attributable to a Party's breach of the Data Processing Agreement and remains subject to the liability caps set out in Article 12 of the Agreement. Article 12.1 of the Data Processing Agreement will be replaced by the following: "If either Party fails to comply with its obligations under this Data Processing Agreement, that Party shall be liable for the direct loss or damage suffered by the other Party to the extent such loss or damage is directly caused by that Party's breach of this Data Processing Agreement. Direct loss or damage will in any case be understood to include, but not exclusively, the costs incurred in connection with having to recompile files of lost or destroyed Personal Data and the costs incurred to prevent or limit loss or damage. Liability with regard to reputation damage and/or loss of profit is excluded. Liability under this Data Processing Agreement shall be subject to the financial liability caps set out in Article 12 of the Agreement."
56	Standard Form - Requirements Compliance – A26	Does this requirement include the need to access multiple DCSs in the same session	Yes, also through a back-office virtual desktop multiple DCSs must be in use concurrently from the same PC. E.g. a handler's employee doing flight closure activities for multiple airlines at the same moment.
57	Appendix 2b - Requirements – B2 IT Infrastructure	With reference to requirement B15, can EANV confirm that a locally installed Windows 11 management workstation, for administration, monitoring, and maintenance purposes is not considered an on-premise server under this requirement. This could be a physical machine or installed on the EANV virtual platform.	If the machine is installed on the EANV virtual platform, it is considered an on-premise server under requirement category B2.
58	Standard Form - Pricing sheet	Can EANV provide more details on how Implementation costs (inc: professional services) will be evaluated, as only hourly rates are requested in the Pricing sheet. Further, in Annex 3b - EANV_General_Purchase_Conditions_IT___Systems_-_Special_Provisions_Professional_Services, Articles 4.2 and 4.3 refer to charging for professional services on an hourly basis. Can EANV please clarify what calculations will be used for evaluating these charges.	Professional services as part of implementation must be covered in the section "Implementation (one-off)". The hourly rates are not part of the calculation the Total Tender Price and are only requested for contractual/future purposes.
59	Annex 3b - EANV_General_Purchase_Conditions_IT___Systems_-_Special_Provisions_Professional_Services – Article 6 Replacement Consultants	Could the Customer confirm that a request to replace a Consultant under clause 6.2 will be based on reasonable, written grounds (e.g. documented underperformance, failure to meet the agreed role requirements, or a material conduct/compliance concern) rather than at sole discretion, and that the Supplier will first be given the opportunity to address the concern?	A request to replace a Consultant will always be a careful, well considered decision by EANV. We can confirm that we will first give supplier the opportunity to address and improve the situation. However, it remains to EANV's sole discretion to deem this addressing and improving as sufficient or not, and to request replacement. The article remains unchanged.

60	Annex 2 - EANV_General_Purchase_Conditions_IT___Systems_-_General_Provisions – Article 6 Access EANV	Can EANV please clarify that no direct costs will be incurred by Supplier from EANV for the provision of any required training, issue of passes or other activities related to obtaining access.	EANV will not charge any costs for obtaining access. For clarity, if background security screening is required, as per the Access policy of EANV, Supplier is responsible for initiating this screening process with the Dutch government. Costs can be incurred by the Dutch government for this screening process. The Access policy of EANV can be found here: https://www.eindhovenairport.nl/en/work-safely We will also insert the Access policy as an Annex to the Agreement.
61	Appendix 2a - Schedule of Requirements – Ch 4 Project Planning	In meeting the target for the first workstation to be setup for testing, does EANV accept that there will be dependencies on each of the airlines in scope, including for establishing connectivity and for testing activities and that Supplier cannot be held responsible for any delays caused by airlines.	Yes we understand. For the initial phase of the test workstation deployment, airline connectivty is preferred, but not a mandatory requirement. Obviously, airline connectivity must be in place when we start formal Acceptance Tests.
62	Annex 2 - EANV_General_Purchase_Conditions_IT___Systems_-_General_Provisions – Article 7 Delivery	Clause 7.3 broadly entitles the Customer to carry out repair/replacement work at the Supplier's cost. Could the Customer please consider amending the clause so that "The Parties shall agree a plan for remediation" in the first instance, with any step-in right applying only if the Supplier fails to remedy, and only where the failure is solely and directly attributable to the Supplier, after written notice and a reasonable remedy period (no less than 30 days)? Could it also confirm any such costs must be reasonable, evidenced, and within the limitation of liability?	Article 7.3 is tight to the situation that the Supplier is not to be able to timely or properly perform its obligation.
63	Appendix 2b - Requirements – A2. Workstations and peripherals	With reference to requirement A20, can EANV confirm, the local applications that are requird for daily operations, are listed in section 4. Software of Appendix 2a - Schedule of Requirements?	Yes, the current list of applications is described in section 4 of Chapter 2 of Appendix 2a. Obviously, the list of local applications may change over time throughout the term of the agreement and will be handled by change requests submitted by EANV to supplier.
64	Appendix 2b - Requirements – A2. Workstations and peripherals	With reference to requirement A26 and A27, can EANV please clarify whether the use of virtual desktop technology is a mandatory solution requirement, or whether alternative technologies that provide equivalent functionality, security, and user experience for accessing PPS back-office functions would also be considered acceptable?	It is not mandatory but a high priority requirement. We are looking for modern solutions to enable PPSs in the back office in such a way we don't have to work on additional computers apart from their corporate pc. Additional computers is not sustainable, not user-friendly, not resource-efficient and not cost-effective.
65	Appendix 2a - Schedule of Requirements, Ch.1 §4.A 'Existing CUPPS installation', p.5 and Ch.2 §1 'Facts and figures', p.6; Appendix 2b - Requirements, ID A12-A17 , pp.1-2 , A21–A25.	Please confirm the final CUPPS workstation inventory, including the quantities for each workstation type, and provide the required configuration for each position. This should include the applicable hardware and peripherals, such as PCs, monitors, keyboards, barcode or boarding pass scanners, boarding pass or receipt printers, bagtag printers and document printers for check-in, gate, service desk etc.	The 38 physical CUPPS positions comprise: • Test workstation: 1 position • Manual check-in workstation: 14 positions • Gate workstation: 13 positions • Service desk workstation: 9 positions • Baggage control room: 1 position • Back-office: 6 concurrent users Exact peripheral configuration per work station is described in the Requirements. Participant must advise on spare parts in its Tender on top of the quantities stated above.
66	Appendix 2a - Schedule of Requirements, Ch.1 §3 'Temporary airport closure', p.5; Appendix 2b - Requirements, ID C1, C7, C8 , p.6; Tendering Guide, §1.3.2 'Out of scope', p.4 (no provisions on delivery, unloading, staging or storage identified)	Access, logistics, and storage. Please clarify what site access, delivery, unloading, staging, and temporary storage arrangements will be made available to the supplier during the implementation period.	Supplier is responsible for implementation, which includes delivery, unloading, staging etc. Any resource (either human, IT or physical location) that EANV needs to provide must be described in the Solution design and Implementation plan (AC3).
67	Appendix 2b - Requirements, ID E17, p.12; Appendix 2a - Schedule of Requirements, Ch.2 §5.A 'WAN connectivity', p.10; Appendix 2b - Requirements, ID B9-B13 , p.4	Remote access and support connectivity. Please confirm the permitted method for secure remote access for support and maintenance purposes, including any restrictions relating to authentication, logging, monitoring, or airport security tooling.	Multiple methods are supported. Depending on the exact implementation of support processes, EANV and supplier will decide on the best method for remote connectivity, subject to the requirements and risks following the Security Annex and Business Impact Analysis. Note that remote connectivy may be subject to change, as security standards and best practices evolve over time.
68	Appendix 2a - Schedule of Requirements, Ch.2 §4 'Software' (A. Airline applications, B. Handler applications, C. Airport applications), pp.8-10; Appendix 2b - Requirements, ID A41-A48 , p.3	Third-party interface scope. Please clarify the full list of third-party interfaces in scope for implementation, migration, validation, or support, including any dependencies on airport or airline systems.	Please refer to Appendix 2a, containing detailed overviews of all applications that must be available on a CUPPS workstation.
69	Appendix 2b - Requirements, ID A48 , p.3; and ID C3 , p.6	Interface ownership and coordination. Please confirm which party will be responsible for coordinating technical engagement with airlines and third-party system providers during implementation, testing, and migration.	The CUPPS system is formally owned by EANV. EANV is therefore in charge regarding the system and interfaces. We have direct relations with all parties involved, e.g. airlines and handlers. However, typical CUPPS providers have close collaborations with airlines, which should be leveraged when beneficial.
70	Appendix 2a - Schedule of Requirements, Ch.4 'Project planning', p.13; Appendix 2b - Requirements, ID C5, p.6	Detailed implementation phasing. Please confirm the expected implementation phasing during the airport closure period, including any area-by-area sequence, access milestones, and mandatory completion dates.	The mandatory milestones / dates are mentioned in the Tendering Guide (and appendices). It is up to Participant to submit an Implementation plan as part of its Tender.
71	Appendix 2a - Schedule of Requirements, Ch.4 'Project planning', p.13; Related Appendix 2b requirements: C1–C8.	Delay caused by third parties. Please clarify how implementation delays caused by third-party dependencies or airport-provided works will be managed contractually and operationally, including any expected replanning process.	Where a delay is caused by circumstances attributable to third-party dependencies that are demonstrably beyond the reasonable control of the Supplier, the Parties shall consult in good faith regarding the impact on the project planning and any appropriate mitigation measures. If such circumstances materially affect the agreed implementation schedule, the Parties may agree on a revised planning, provided that the Supplier has promptly notified EANV of the relevant circumstances and has taken all reasonable steps to mitigate the impact of the delay. For the avoidance of doubt, the Supplier shall not be liable for any delay, failure to meet a milestone, or failure to achieve the agreed go-live date to the extent such delay or failure is solely and directly caused by circumstances beyond the Supplier's reasonable control and sphere of influence, provided that the Supplier has complied with its notification obligations and has taken all reasonable measures to prevent, mitigate and overcome the consequences of such circumstances. Circumstances attributable to the Supplier's subcontractors, affiliates, agents, or other third parties engaged by or on behalf of the Supplier shall not constitute third-party dependencies for the purpose of this Article and shall remain fully within the Supplier's responsibility.
72	Appendix 2b - Requirements, ID C9-C19 , pp.6-7; Appendix 2a - Schedule of Requirements - Ch.1 §3 'Temporary airport closure' (ORAT phase), p.5 and Ch.4 'Project planning', p.13	The acceptance plan, on-site testing, independent penetration testing and requirement for acceptance by 1 June 2027 are understood. Please confirm the acceptance governance, stakeholder approval responsibilities, required airline or DCS validation, ORAT coordination and formal sign-off procedure.	As per requirement C9, Participant shall develop an acceptance plan that contains test plans to validate the implementation. Required airline and DCS validation will be coordinated by EANV (we will involve handlers into the acceptance tests). Formal sign-off is done by EANV (by Product Owner Airport & Passenger Systems or a delegated person).
73	Appendix 2b - Requirements, ID C15, p.7; ID C21-C23 , p.7	Documentation deliverables. Please clarify the minimum documentation set expected from the supplier, including HLD, LLD, installation records, as-built documentation, operating procedures, support procedures, and handover documents.	The documents we expect the Supplier to submit: High-level design, low-level design, installation records, as-built documentation, operating procedures, support procedures, and handover documents.
74	Appendix 2b - Requirements, ID D21, D28 , p.10; ID B44, p.6	Spare parts storage and ownership during operations. Please confirm where spare parts are expected to be stored during the support period and whether the airport has any requirements regarding ownership, replenishment, or minimum stock levels. Airport will manage them and will be responsible to ask for replacement.	Spare parts will be bought, owned and stored by EANV. We do ask Supplier to validate spare parts as part of the half-yearly health check and to advise EANV on what spare parts to keep on stock, based on fail rates, time required to replace, EOS/EOL notifications by manufacturers etc.
75	Appendix 2b - Requirements, ID D36-D37, p.10; ID D24-D28 , p.10	Service reporting and governance. Please confirm the required frequency and format for service reports, KPI reviews, incident trend reporting, and formal service review meetings, noting that quarterly written reporting is understood to be required.	Requirement D37 demands a quarterly report. Other service governance details will be discussed and adjusted throughout the term of the agreement, as it depends on the Suppliers actual performance.
76	Appendix 2b - Requirements, ID E1, ID E12, E18-E19 , pp.11-12	Applicable cybersecurity policies and standards. We understood that the solution must comply with the EANV Security Annex throughout the contract. The requirements also refer to zero trust, least privilege, VLAN segmentation, encryption, hardening, monitoring, vulnerability management, ISO 27001 and CIS benchmarks. However, the actual Security Annex is not available in the project documents reviewed. Can you provide it?	The Security Annex is enclosed as Annex 9 of the Agreement. Please make sure to open the ZIP file, as published on TenderNed.
77	Appendix 2b - Requirements, ID E7, E9, E10, E16 , pp.11-12	Endpoint security and hardening. Please confirm the expected requirements for operating system hardening, anti-malware or EDR tooling, patch management, vulnerability remediation, and security logging.	The requirements are outlined in Appendix 2b.
78	Appendix 2a §1 Facts (p.6) vs Appendix 2b A41–A46 (A3 PPS); Appendix 2a §4A	The Facts & Figures list 10 airlines while A41 names 7 carrier codes (4 airline groups). Please provide the definitive list of airlines and their DCS/Passenger Processing Systems with software versions that must be certified on the solution (e.g. Navitaire GoNow, Navitaire SkySpeed, Res2 iPort, Aerocloud eDCS, Pegasus, SunExpress). Please also confirm whether EANV or the airlines provide test access and coordinate certification, and the expected lead time per application.	The airlines are listed in requirement A41 and A46. We cannot provide exact version numbers as there may change over time throughout the term of the agreement. EANV will coordinate with the airlines and handler to arrange test access. Certification (if applicable) must coordinated by the Participant itself.
79	Appendix 2b A41–A44 (A3 PPS), p.3	For the Critical PPS support requirements (A41–A44, which allow only a Compliant/Non-compliant response), please confirm whether the required PPS support and certification must be demonstrably in place at Tender submission or by the acceptance date.	It must be in place at Tender submission. Regarding A41: All airlines listed in A41 currently use Navitaire GoNow as a native DCS.
80	Appendix 2a §4C (Airport applications)	Please confirm the AODB and gate-client product in use (Airport Hive) and the required integration scope with the CUPPS solution (e.g. flight-data feed and gate client), and whether any interface development is within the scope of this Engagement.	Only the AODB gate client must be available on the CUPPS workstation. This is a browser-based web client. No specific interface is required.
81	Appendix 2b A49 & A50 (A4 Data, reporting and integration)	A49 and A50 give ActiveMQ and HTTP API as examples for the real-time boarding-pass and bag-tag data feed. Please confirm the required target interface (ActiveMQ topic and/or HTTP API), the message format, and which party owns and provides the receiving endpoint.	EANV currently owns and provides an API (called EventAPI) that allows for third parties to POST (real-time) events to. An example message is included below. { "IRMEvent": { "Event": "IsProcessedAt", "Subject": "Passenger", "Object": "TouchPoint", "EventProperties": { "Type": "IsProcessedAt", "WhenDateTimeStamp": "2026-01-01T10:27:00+01:00" }, "SubjectProperties": { "Type": "Passenger", "Properties": [{ "Label": "PNRCode", "Value": "V99M4Z" }, { "Label": "Checkin Sequence Number", "Value": "0009" }, { "Label": "OperatingCarrier", "Value": "XX" }, { "Label": "FlightNumber", "Value": "9999" }, { "Label": "FlightDate", "Value": "2026-01-01" }] }, "ObjectProperties": { "Type": "TouchPoint", "Properties": [{ "Label": "TouchPointID", "Value": "ABC123" }, { "Label": "BusinessActivityDescription", "Value": "Testing" }, { "Label": "TouchPointType", "Value": "S" }, { "Label": "BusinessActivityCode", "Value": "08" }] } }, "MessageID": "95a7ea0f-a50a-0af5-e053-15c416acbdf0", "OriginatingAirport": "EIN", "SourceSystem": "TestEIN", "Version": "5.4"}

82	Appendix 2a §3D (Baggage control room); Appendix 2b A15	Please confirm the Baggage Handling System (BHS) and Baggage Reconciliation System (BRS) at the baggage control room, including product name and required message standard (e.g. BSM/BPM per IATA RP1745), and whether BHS/BRS interface development is within the Participant's scope. Please also confirm how many baggage control room workstations are required (A15 is Critical but not itemised in the 38 positions) and whether they are additional to the 38.	One workstation is required for the baggage control room. BHS/BRS interface is out-of-scope. The airline/DCS is responsible for sending BSMs.
83	Tendering Guide §1.3.1 Scope, p.4; Appendix 2a §1, p.6	The scope lists 38 positions (1 test, 14 check-in, 13 gate, 10 service desk). Service desk shows 10 in scope yet Appendix 2a lists 11 service desk positions (incl. 1 arrivals and 2 PRM). Please confirm the definitive number of service desk workstations and the position-type breakdown to be priced and delivered.	Apologies for any confusion caused. The PRM Assistance desks (as part of the service desk count in Appendix 2a) do not require CUPPS workstations. For the final numbers, refer to the answer to Question 65.
84	Appendix 2b A17, A26, C28 (back-office VDI); Appendix 2a §3E	Please confirm: (a) the expected number of concurrent back-office VDI users, to size concurrent/pooled licensing; (b) that back-office access will continue from handler-owned PCs via virtual desktop technology as in the current architecture; (c) whether the Participant must provide the VDI platform and on whose hardware the back-office virtual desktops execute (EANV hypervisor vs handler PCs); (d) whether management of handler endpoints is in scope; and (e) whether these positions are additional to the 38.	a. We expect a maximum of 6 concurrent back-office users. b. Ideally yes, third-party PCs c. Supplier must provide the virtual desktop infrastructur, but may rely on EANV's hypervisor if it is within the limits set out in the requirements. d. The Supplier must provide installation instructions and support the VDI user experience, but does not need to manage the handler-owned PC. e. Yes, there positions are additional to the 38.
85	Tendering Guide §1.3.1 Scope ('Spare parts'), p.4	Spare parts are included in scope but not quantified. Please specify the spare-part set to be included in the base offer (quantity per component type), or confirm the Participant may propose it and describe how it will be evaluated.	The Participant should submit a spare-parts proposal based on its experience with projects of this type.
86	Appendix 2a §1 Facts (self-service bag drop), p.6	12 self-service bag-drop units are installed at check-in positions 1–12 and self-service bag drop is out of scope. Please confirm whether the CUPPS solution must interface/integrate with these existing units and, if so, the required interface and responsible party.	No, CUPPS and Self-service bag drop run fully isolated.
87	Appendix 2b A18 (A2 Workstations and peripherals)	Please confirm the maximum number of Passenger Processing Systems expected to be open simultaneously on a single workstation, so the workstation and platform can be correctly sized.	At max. 5 PPS will be open simultaneously.
88	Appendix 2b A9 & A39 (A2 Workstations and peripherals)	Please confirm whether EANV requires specific makes/models of peripherals (boarding-pass printer, bag-tag printer, document printer, scanner, boarding gate reader, swipe/OCR keyboard), or whether the Participant may propose its own certified peripherals meeting the stated requirements.	The Participant may propose its own certified peripherals meeting the stated requirements.
89	Appendix 2b A33 (A2 Workstations and peripherals)	A33 asks that the gate workstation be expandable to support two self-boarding gates in future. Please confirm that self-boarding gate hardware is out of scope for this Engagement and required only as a future-expansion capability of the gate workstation design.	Correct. It is out-of-scope of this engagement. It is purely required as a future expansion capability.
90	Appendix 2b A22 (A2 Workstations and peripherals)	Please confirm that the required boarding-pass scanning performance is a minimum of 20 scans per minute per workstation, and that scanning of a barcode from a mobile phone is required at both check-in and gate positions.	Correct.
91	Appendix 2b A19 (A2 Workstations and peripherals)	Please confirm the expected lock/unlock behaviour: that on unlock the agent resumes all previously open airline applications without re-authenticating to each, and confirm the airport's preferred lock/timeout values.	Correct. We intend the same thing as 'locking' on a Windows PC. The exact auto-lock timeout value will be discussed and configured as part of implementation.
92	Appendix 2b B9 & B10, p.4 vs E4 & E13, p.11–12	B10 states the solution shall contain no Participant-provided network switch and B9 uses EANV's Layer-2 services, while E4 requires VLAN segmentation inspected by a next-generation firewall and E13 states the firewall 'should' be provided by EANV. Please confirm which party provides and manages the firewall and VLAN segmentation, that firewall rule changes follow an EANV change-management process, and that the Participant is not expected to supply any network hardware.	Layer-2 networking must be delivered by EANV (as per requirements B9 and B10). Also, EANV prefers to deliver the firewall (requirement E13) for inter-VLAN and WAN traffic, however this is not mandatory. Participant is permitted to design a solution where he delivers a firewall cluster.
93	Appendix 2b B9–B13 (B2 IT infrastructure); Appendix 2a §5; Tendering Guide §1.3.2	Please confirm that EANV provides all Layer-2 switching, structured cabling and a live 1 Gbps data outlet at each CUPPS position, and that no cabling or electrical work is within the Participant's scope.	Correct, EANV will provide that.
94	Appendix 2b B14 & B18 (B2 IT infrastructure); B15	B14 requires any on-premise servers to run on the EANV hypervisor while B18 states the solution should not require any local server. Please clarify EANV's preference between (a) on-premise virtual servers on the EANV hypervisor and (b) a no-local-server solution, confirm both are acceptable, and confirm that the 12 vCPU / 48 GB RAM / 240 GB HDD envelope (B15) is the hard maximum and whether it applies to the solution as a whole.	Both are acceptable, but EANV prefers a solution that does not require local servers, as per requirement B18. The envelope is a hard maximum and applies to the solution as a whole. In case more resources are required, make sure to an actual proposal in the next round of question.
95	Appendix 2b B14–B17 (B2 IT infrastructure)	If on-premise virtual servers are used on EANV's hypervisor, please specify the hypervisor platform and version, and confirm whether the Participant will have direct management access to its own virtual machines.	The hypervisor is Broadcom/VMware vSphere ESX 9. Remote management details will be discussed during implementation. Supplier can have direct management access to the virtual machines. For clarity: Supplier will not have access to vSphere. In case Participant requires VM to be restarted or reconfigured through vSphere, the EANV IT servicedesk can be contacted.
96	Appendix 2b B17 (B2 IT infrastructure); D29 & D30 (Business Continuity)	B17 states EANV backs up the on-premise servers to two locations. Please confirm the backup frequency, retention and recovery capability EANV provides, so the Participant can align with the D30 recovery objectives (RTO 4 hours, RPO 8 hours).	The back-up infrastructure of EANV is sufficient to meet the recovery objectives.
97	Appendix 2b B13 (B2 IT infrastructure)	Please confirm the minimum functions expected to continue in offline/degraded mode during a loss of EANV-provided internet (e.g. check-in and boarding on local operation), and whether a store-and-forward mechanism is required for external interfaces once connectivity is restored.	A handler should be able to use an emergency local login mode to enter CUPPS. Any airline that has its own WAN DCS connection into Eindhoven Airport (e.g. via SITA AirportHub) should not be affected by the internet outage. For background: In case EANV provides firewalling, if the primary internet connection fails, we will fall back our secondary (or tertiary) internet connection. Therefore the probability of an internet failure is limited.
98	Appendix 2b D3, p.7 & B13, p.4	The solution must achieve at least 99.9% availability per calendar month, while EANV provides the internet (99.95%), network, firewall, hypervisor and power. Please confirm that downtime caused by EANV-provided infrastructure or by third parties is excluded from the Participant's availability calculation.	Downtime that is caused by EANV-provided infrastructure is excluded from the downtime calculation. All other causes are not excluded. For clarity: Downtime caused by third parties that operate as subcontractor of Participant, e.g. a cloud hosting provider such as AWS or Azure, are not excluded and are the responsibilty of the Participant.
99	Appendix 2b B22 (B3 Performance)	Please confirm that the 90-second workstation readiness target is measured from cold power-on to ready-for-login, and confirm the reference test conditions (e.g. first boot after power loss vs normal restart).	Correct; Cold boot (=power button push) until ready-for-login (= CPU and Disk IO are stable after boot processes have loaded).
100	Appendix 2b B6 & B7 (B1 Standards and compliance)	B6 (Critical) and B7 (High) appear near-identical (deletion of personal data in log/debug files within 2 months). Please clarify the intended distinction between them (or confirm B7 is redundant), the exact retention/deletion period, and whether automatic deletion is mandatory for all data sources that may hold personal data.	The requirements are not redundant. B7 explicitly states that personal data should be deleted "automatically".
101	Appendix 2b (Service and support section), p.10	The requirement IDs skip from D22 directly to D24 (no D23). Please confirm that no requirement is missing between D22 and D24.	Apologies, D23 is only missing in numbering. No requirement is missing.
102	Appendix 2a §5C (Airline connectivity)	Two airlines are currently connected via the incumbent CUPPS provider's data centre and must be replaced during deployment. Please confirm which two airlines are affected, the target connectivity method (SITA AirportHub, local ISP, or EANV-provided), and the responsibility split for making the change.	It concerns Ryanair and TUI. Target connectivity method will be decided upon during implementation phase, depending on the options available.
103	Appendix 2b D42 (D4 Monitoring and alerting)	Please confirm EANV's central monitoring and alerting platform and the required integration method (SNMP and/or API), so the CUPPS solution can be integrated into EANV's central monitoring.	EANV runs a generic central monitoring platform that is capable of consuming different types of end points. We will adapt to the standard integration options of the CUPPS platform.
104	Appendix 2b D39 & D40 (D4 Monitoring and alerting)	Please confirm whether the real-time monitoring platform must be provided by the Participant or integrated into an existing EANV tool, and confirm the required scope of consumable/peripheral alerts (e.g. toner low, paper low, peripheral disconnect).	Preferably it is integrated into EANV's tooling, monitoring platform and/or servicedesk software. If that is not an option Participant may opt to provide a platform. EANV would like to understand all alert types that can be enabled/configured. At least the following alerts should be configured: Toner low, toner empty, peripheral down (incl. which peripheral), PC down (incl. reason), printer error (incl. reason). It should also be possible to reboot a work station remotely through the monitoring platform. It should also be possible to remotely connect to a workstation (e.g. VNC based solution) to monitor a workstation.
105	Appendix 2a §2 Teams, p.7; Appendix 2b D5, D13, D15, p.7–9	First-line support is by EANV, but TS&FM is on-site only 06:00–21:00 and D&IT works business hours (with an on-call operator for P1/P2). Please clarify how the Participant is expected to meet the P1 target (response ≤30 min, resolution ≤4 h, 24/7) for incidents requiring on-site action between 21:00 and 06:00, whether a defined on-site dispatch response time applies, and whether a permanent local presence is expected.	Before 6:00 and after 21:00 only an Airport Operations Manager is on duty. Participant must propose a service model that supports our operational model and must align its proposal with the skills and duties of the available staff.
106	Appendix 2b E5 & E8 (E1 Cyber Security)	E5 and E8 are marked Priority '1. Critical' (knock-out) yet worded with 'should'. Please confirm whether these are genuinely knock-out. For E5 (handler identity-provider federation), please confirm the handler IdP(s) to integrate (e.g. Entra ID, OAuth, SAML 2.0), which handler operates them, and whether federated login is required at go-live or may be delivered before acceptance.	Apologies, both requirements are worded incorrectly and should use "shall". Both requirements are knock-out requirements. The handler (Viggo) runs Microsoft Entra ID IdP. Integration must be delivered as part of system acceptance.
107	Appendix 2b E11 & E15 (E1 Cyber Security); Annex 9 Security Annex	24/7 security monitoring (E11) is Critical while SIEM integration (E15) is only High. Please confirm whether the 24/7 security monitoring (SOC and SIEM) is operated by EANV, by the Participant, or shared, where responsibility for alert triage and first response sits, and the responsibility boundary between the CUPPS solution components and the EANV enterprise security environment.	It is mandatory that Participant has security monitoring in place, as per requirement E11. The integration into EANV's SIEM platform should only cover a selection of events that will be agreed upon during implementation.
108	Appendix 2b E12 (E1 Cyber Security); Annex 9 Security Annex §8.1, p.7	Please confirm the vulnerability-remediation timescales by severity in the Security Annex that will apply to the CUPPS platform (Critical internet-facing = 48 hours). Given internet access is provided centrally by EANV and the solution sits behind EANV's firewall, please clarify which components EANV considers 'internet-facing' for these timelines.	Internet-facing means that there is an inbound firewall rule enabling inbound traffic reaching the device or machine. Please note that a Participant may opt to install its own firewalls, which we consider as an internet-facing device.
109	Appendix 2b C13 (C2 Acceptance and go-live)	Please confirm the scope and target of the independent penetration test (e.g. whether the single test workstation due 1 March 2027 is the test target), the expected test window and retest process, the remediation window relative to the 1 June 2027 acceptance date, and which party bears the cost of any required re-testing to close Critical/High findings.	Please see answer to Question 8. Furthermore, we can confirm the test workstation is the test target (including underlying systems/infrastructure). EANV aims to execute the penetration test during the first week of March. Depending on the amount of findings, we expect the test report to be available shortly after. The cost for the first round of retesting will be covered by EANV. If more restests are required, the costs will be charged to the Supplier.
110	Appendix 2b C16 (C2 Acceptance and go-live); Appendix 2a Ch.4; Tendering Guide §8.4	Acceptance/go-live is required by 1 June 2027 during the airport closure, when airlines are not operating. Please confirm the network, server and airline-DCS access available for the single test/exploration workstation by 1 March 2027, EANV's target dates for provisioning the Layer-2 network, internet, firewall and hypervisor dependencies, and how end-to-end acceptance testing of live airline DCS/PPS connectivity will be validated during the closure (test environments, test data or airline participation EANV will facilitate).	We ensure that the availability of EANV facilities, i.e. networking, hypervisor, firewall rules, will be delivered on-time, provided that Supplier has set out a clear planning and implementation plan. EANV currently has a test environment for almost every DCS available. EANV can (and will) engage the handler and airlines during acceptance testing. Also EANV can coordinate with one or more airlines to perform a production test in a production DCS upon final acceptance testing.

111	Tendering Guide §1.2, p.3–4 vs Security Annex §2.2, p.5	§1.2 states no governmental screening is expected during the airport closure, whereas the Security Annex requires a VGB (Verklaring van Geen Bezwaar) for staff/third parties accessing high-privileged accounts, critical systems or sensitive information. Please confirm whether VGB screening will be required for the Participant's 2nd/3rd-line and administrative personnel after airport re-opening and for the remainder of the contract.	During airport closure, no airport area is marked as secured area, which means that physical access to the airport premises does not require governmental screening. This is indeed unrelated to the screening requirements set out in the Security Annex for high-privileged accounts. However, we suggest to discuss reasonable screening requirements after contract awarding for privileged support staff.
112	Security Annex §1.3, p.4; Tendering Guide §2.10.5, p.10	The documents prohibit processing EANV confidential/sensitive data in generative-AI or external AI platforms without prior written consent. As modern support/monitoring tooling is often cloud-based, please clarify whether operational data such as system logs, telemetry and monitoring data that the Participant must process in its own tooling falls within this restriction, and the process for obtaining consent.	Yes, these types of data fall within the restriction, particularly because log data may contain personal data.
113	Appendix 1 Agreement §6.7 (p.7); Pricing sheet header; Tendering Guide §1.4	The pricing sheet states prices are fixed to 31-12-2027 with indexation possible from 1-1-2028, whereas Agreement §6.7 permits indexation only after the Agreement has been renewed for the first time (i.e. after the initial 5-year term), capped at 5% of the CBS Business Services turnover index. Please clarify what 'FA/DA' refers to, reconcile these provisions, and confirm from which date and on what basis the recurring rates may be indexed.	"FA/DA" is a typo and must be read as "Agreement". See answer to Question 22 for the complete answer and refer to version 2 of the Pricing Sheet.
114	Standard Form Pricing sheet, 'Hourly rates / Mark-up rates' section	The mark-up line labelled 'Out of business hours (08:00–18:00 CET)' appears mislabelled. Please confirm the intended business-hours window and the time periods to which the out-of-hours, Saturday and Sunday/public-holiday mark-ups apply.	We removed the pre-filled items under 'Mark-up rates' allowing Participant to fill these himself. Please refer to version 2 of the Pricing Sheet.
115	Agreement Annex 5 / §6.1 (p.11); Appendix 2a Ch.4	Acceptance/go-live is targeted for 1 June 2027, while full operational use begins at airport re-opening on 19 July 2027. Please confirm the exact trigger date for commencement of recurring-fee invoicing.	We expect go-live at 1 June 2027. EANV considers it fair that Supplier is allowed to start recurring-fee invoicing from that date.
116	Agreement §12.1 / GPC Art 18.2 (p.9); SR2 (p.16)	Supplier liability appears capped at EUR 500,000 per event / EUR 1,500,000 per year for an up-to-8-year (5+3×1) critical passenger-processing contract. Please confirm whether this cap has carve-outs for data breach/GDPR non-compliance, IP infringement, wilful misconduct or gross negligence, or whether it is an all-inclusive cap.	See answer to questions 27, 50, 51 and 55.
117	Agreement §5.2 & §8.3 (pp.6–7)	Please confirm whether the stated penalties are the Supplier's sole and exclusive remedy for the relevant breach (liquidated damages), or whether EANV may claim additional (uncapped) damages beyond the stated penalty caps.	See answer to questions 20 and 23.
118	Agreement §6.6 (p.7)	§6.6 allows EANV a 5% discount if an invoice is submitted more than 4 months after the Delivery Date. Please confirm whether this applies per invoice or in aggregate, and whether it applies to recurring/annual invoices or only one-off milestone invoices.	This applies to any form of Delivery. Recurring/annual invoices should be sent in advance, so practically it would only apply to one-off milestones.
119	Agreement Annex 5 Payment Schedule (p.11)	If a P1/P2 incident occurs during an acceptance/milestone window due to causes outside the Supplier's control (e.g. EANV infrastructure failure or third-party airline outage), please clarify whether the milestone clock resets, whether the related milestone payment can be delayed, and the treatment of such external-cause events.	If such an event occurs and materially affects planned activities such as acceptance testing, the Parties will discuss and agree any reasonable impact on the project timeline and milestones.
120	Tendering Guide §8.2 AC1 Price (p.22)	Please confirm whether the 'Total Tender Price' used for AC1 scoring covers only the 5-year firm term, or also incorporates the value of the 3 optional 1-year extension periods.	The Total Tender Price will be taken exactly from the Pricing Sheet, and thus not include the 3 optional 1-year extensions.
121	Tendering Guide §1.4 (p.4); Agreement §3.1	Please confirm the pricing/rate basis for the 3 optional 1-year extension periods — i.e. whether extension-year pricing is at the original Tender rates (subject to §6.7 indexation) or subject to renegotiation when each extension is exercised.	Conditions shall remain unchanged if the Agreement term is extended. For clarity, article 3.1 of the Agreement shall be replaced by: This Agreement shall enter into force on 1 January 2027 and shall terminate by operation of law on 31 December 2031. EANV is entitled to unilaterally extend this Agreement, on the same terms and conditions, for periods of 1 year, with a maximum of 3 extensions. EANV shall inform Supplier of its intention to extend the Agreement no later than one month before the end of the term.
122	Appendix 2b B15/B16 (p.4); Appendix 2a Ch.2 §6	B15/B16 require any virtual-server software licensing (incl. upgrades/updates) at no additional cost. Please confirm whether this no-additional-cost obligation extends to the fictitious pricing add-on in Appendix 2a §6, or whether that fictitious amount is purely a scoring mechanism with no cash-flow implication.	The fictitious amounts for on-premise virtual servers is purely a scoring mechanism. Requirement B16 concerns software that the Participant installs on virtual machines provided by EANV. The Participant must ensure all software on the virtual machines is properly licensed, except for Microsoft Windows Server 2025 Datacenter. Example 1: If Participant wishes to deploy a virtual machine that runs an OS that requires a paid license, such as SUSE Linux Enterprise, this license must be covered by Participant. Example 2: If Participant wishes to deploy a virtual machine that runs Windows Server 2025 Datacenter edition, the VM can be licensed through EANV's core-based Windows Server 2025 Datacenter license.
123	TenderNed Publication (p.2) vs Agreement §3.1 (p.5)	The TenderNed notice states a contract 'Duration end date' of 31/12/2034, while Agreement §3.1 states termination by operation of law on 31 December 2031, extendable by up to 3×1 year (i.e. max 2034). Please confirm the correct base (firm) contract end date for financial modelling: 31 Dec 2031 or 31 Dec 2034.	TenderNed reflects the maximum possible contract end date and includes the optional extension periods of 3x1 year.
124	Reserve Contractor Agreement (Appendix 3) §3 (p.3)	§3.1 confirms no fee is payable for maintaining the Tender under the Reserve Contractor Agreement for the 6-month standstill period. Please confirm whether the rates held open are the original Tender rates without escalation, irrespective of how much of the 6-month standstill has elapsed before the option is invoked.	As per article 1.2 of the Reserve Contractor Agreement: "1.2Tenderer shall maintain its Tender for the duration of this Agreement."
125	Tendering Guide §2.7 (pp.7–8)	Please confirm the applicable VAT/tax treatment for a non-Dutch (foreign) prime bidder — specifically whether reverse-charge VAT applies and whether the Total Tender Price should be quoted inclusive or exclusive of Dutch VAT.	All pricing must be excluding VAT.
126	Agreement §6.2 (p.6)	Please confirm the currency in which invoices, fees and the Total Tender Price/Pricing Sheet are to be denominated and settled, and whether any FX risk-sharing or currency-adjustment mechanism applies for a non-Eurozone prime bidder.	As per article 4.1 of GPCITS General Provisions (Annex 2 of the Agreement), prices are in EUR.
127	ARN2016 §15.1 (p.8); Tendering Guide schedule (p.5)	Please confirm the Tender validity period applicable to this procurement and whether an extension request should be anticipated.	Please refer to article 14 of ARN (Appendix 4). Currently there is no indication that an extension request should be antipated.
128	Tendering Guide §5.1 SR1 Corporate Guarantee (p.16)	Please confirm the exact Standard Form format/wording of the SR1 Corporate Guarantee, and whether it must be issued and submitted with the Tender or only upon request within 10 calendar days.	The standard form is uploaded to TenderNed as part of this procedure and must be submitted as part of your Tender as per section 2.6 of the Tendering Guide.
129	Tendering Guide §5.1 SR1 & §5.2 SR2 (p.16)	Please confirm whether this tender requires a Bid Bond and/or Performance Bank Guarantee (PBG); if so, the applicable value/percentage and required format/template. Note: the Participant may not have a legal entity or bank account in the Netherlands — please advise in advance any specific local requirements for issuing a Bid Bond or PBG.	No, this is not required. Please refer to the answer to question 19.
130	Agreement §6.2 (p.6); GPC Annex 2 §5	Please confirm the payment term (days from receipt of a valid invoice to payment) under the General Purchase Conditions, as this materially affects working-capital planning for the back-loaded payment schedule under Annex 5.	Payment will be made within 30 days, subject to Article 5 of the GPCITS. Invoices may be submitted in accordance with the payment schedule in Annex 5.
131	Appendix 1 Agreement; Annex 2 (General Purchase Conditions) and Annexes 3a–3d	Please confirm the order of precedence between the CUPPS-specific requirements and SLA (Appendix 2b) and the General/Special Purchase Conditions (Annex 2 and 3a–3d) where they conflict — for example on service credits, warranty duration and limitation of liability.	Please refer to article 2.3 of the Agreement. Based on your question, the following precedence is applicable: 1. Requirements (Annex 1 as part of the Agreement) 2. GPCITS Special Provisions 3. GPCITS General Provisions 4. SLA (as part of the Supplier's Tender) For clarity reasons, we will swap Annex 2 and Annex 3 of the agreement, such that the order to Annexes matches the order of precedence.
132	Tendering Guide §5.5 SR5 Core Competence 2 (p.17)	Core Competence 2 requires a reference airport operating under a regime 'comparable' to the EU (e.g. NIS2, EASA Part-IS). Please confirm whether references from airports outside the EU subject to comparable regimes are acceptable, and how 'comparable' will be assessed.	References outside the EU are acceptable, provided EANV considers the applicable regime sufficiently comparable. Assessment will be on a case-by-case basis. If comparability is unclear, EANV may engage an independent expert.
133	GPC IT & Systems – Special Provisions SaaS §5 Service levels (p.4)	Please clarify the scope of the 'special requirements' EANV may impose on fall-back facilities under §5.2, and the extent of the compatibility obligation with Hardware/Software 'in use or to be used' at EANV, including treatment of material additional cost or implementation impact.	Any special requirement by EANV is (so far) covered in the requirements set out in this procurement.
134	GPC IT & Systems – Special Provisions Software §10 Escrow (p.6)	Please clarify whether §10 applies to third-party Software permitted under §4 where the Supplier does not own or have the legal right to deposit the underlying source code and proprietary materials.	See answer to Question 35.
135	Security Annex v8.0 – Ch.1 About this document – Para B (p.4)	Please clarify (i) who is responsible for conducting/providing the Business Impact Analysis referred to in Paragraph B, and (ii) how cybersecurity requirements identified after contract formation will be addressed where they materially affect the agreed scope, cost or timeline.	EANV will own and lead the Business Impact Analysis, with the Participant providing reasonable cooperation and relevant information. Any additional cybersecurity measures identified after contract formation will be assessed jointly for applicability, proportionality and impact on scope, cost and timeline. EANV expects that most measures will be reasonable, aligned with industry best practices and already covered by a mature cybersecurity framework. Where a measure has a material impact on the agreed scope, cost or timeline, the parties will address it through the applicable contractual change-control process.
136	Data Processing Agreement §13.3 and §14.3 Amendments	§13.3 permits EANV to amend the DPA terms during the term, whereas §14.3 requires amendments to be agreed by both parties in writing. Please confirm that any amendment under §13.3 will require mutual written agreement in accordance with §14.3.	Yes we confirm.
137	General	Please confirm what dates the new airside areas will be available and if there will be any dates with restrictions to acces during the airport closure time	The new airside areas are already available, but the desks (where the CUPPS work station will be located) are not yet installed. Currently, EANV plans to have the physical desks available at the following dates: - Gates new building: 1 February 2027 - Gates existing building: 1 May 2027 - Service desk (Schengen): 1 May 2027 - Service desk (Non-Schengen): 1 May 2027 No rights may be derived from this indicative planning. After contract award, we will closely align with project manager, responsible for the installation of the physical desks. With respect to any restrictions during the airport closure; EANV is still in talk with authorities about the access policy during airport closure regarding Health & Safety requirements. So far, we don't expect any restrictions for Supplier.