DATA PROCESSING AGREEMENT BELONGING TO SSBD UNITS AND THE MAINTENANCE AND SUPPORT

The undersigned:

1. **Eindhoven Airport N.V.,** a private company with limited liability under Dutch law, with its offices on Luchthavenweg 13 and official place of business at Eindhoven, listed in the Commercial Register in Eindhoven under file number 17051407, legally represented in this matter by its Chief Executive Officer (CEO), R.A.J. Hellemons, and its Chief Operations Officer (COO), M.P.J. van den Bogaard hereinafter referred to as "**EANV**"

   and

2. The <**legal form + company name**> with its offices on <address> and official place of business in <place>, listed in the Commercial Register in <place> under file number <Chamber of Commerce/company number>, legally represented in this matter by <name> in the capacity of <function>, hereinafter to be referred to as the "**Data Processor**",

EANV and the Data Processor are hereinafter jointly referred to as the "**Parties**",

WHEREAS:

I. EANV has entered into one or more agreements with Data Processor for the provision of (various) services by Data Processor to EANV, or will enter into such an agreement. This/these agreement(s) are hereinafter referred to as the "**Main Agreement**" and is/are further specified in the title of this Data Processing Agreement.

II. In the performance of the Main Agreement, Data Processor will process data with regard to which EANV is and remains the Controller. These data include Personal Data within the meaning of the General Data Protection Regulation (EU 2016/679), hereinafter referred to as the "**GDPR**".

III. In view of the provisions of Article 28(3) and (4) of the GDPR, the Parties wish to set out the conditions for the processing of such Personal Data in this Data Processing Agreement.

HEREBY AGREE AS FOLLOWS:

1. Subject matter of this Data Processing Agreement

1.1 This Data Processing Agreement (hereinafter referred to as the "**Data Processing Agreement**") applies solely to the processing of Personal Data within the scope of the Main Agreement.

1.2 Terms such as "Processing", "Personal data", "Data Controller", "Data Processor" and "Data Subject" have the meaning ascribed to them in the GDPR.

1.3 It is possible that the Data Processor will process Personal Data on EANV's behalf (hereinafter to be referred to as the "**Personal Data**") in the course of the performance of the Main. Annex 1 contains an overview of the categories of Personal Data and the purposes for which the Data Processor may process the Personal Data.

2. The Data Controller and the Data Processor

2.1 Parties are obliged to comply with the GDPR irrespective of the privacy qualifications attributed to the Parties in this article.

2.2 Pursuant to the applicable law, EANV qualifies as the controlling party – the Controller – in the processing of the Personal Data. EANV has appointed the Data Processor and the Data Processor agrees to process Personal Data on the Controller's behalf.

2.3 The Data Processor guarantees that it will only process the Personal Data based on written instructions from EANV and in such a manner – and insofar – as required for the provision of the services under the Main Agreement, except as required to comply with a legal obligation to which the Data Processor is subject, or to follow instructions issued by EANV. The Data Processor will never process the Personal Data for its own purposes.

2.4 In particular, EANV may give instructions with regard to the retention period of each of the Personal Data referred to in Annex 1 and with regard to the correction, anonymisation, blocking, deletion or any other processing of the Personal Data. The Data Processor will provide all reasonable assistance to enable EANV to comply with its statutory obligations in the event that a Data Subject invoked his or her rights pursuant to applicable law, including the GDPR.

2.5 The Parties are entering into the Main Agreement in order to make use of the Data Processor's expertise in the context of the Main Agreement and the processing of Personal Data for the purposes set out in Annex 1. The Data Processor may exercise its own discretion in the selection and use of such means as it deems necessary to pursue those purposes.

3. Confidentiality

3.1 Without prejudice to any existing contractual arrangements between the Parties, the Data Processor guarantees that it will treat all Personal Data as strictly confidential and that it will inform all its employees, agents and/or data processors engaged by the Data Processor and/or are explicitly approved by EANV (hereinafter referred to as the "**Sub-Data Processors**") and possible third parties of these Sub-Data Processors engaged in processing the Personal Data, of the confidential nature of the Personal Data.

3.2 The Data Processor will ensure that, to that end, such parties have signed an adequate sub-data processing agreement (hereinafter referred to as the "**Sub-Data Processing Agreement**") as specified in further detail in Article 4 of this Data Processing Agreement. The Data Processor will, when there is reason to do so, provide EANV with evidence that his/these Sub-Data Processing Agreement(s) have been concluded.

4. Engagement of Sub-Data Processors

4.1 The Data Processor will refrain from subcontracting any of its activities consisting, in part or in full, of the processing of Personal Data to one or more Sub-Data Processors without EANV's prior written consent.

4.2 The Data Processor will append an up-to-date list of Sub-Data Processors already engaged, as stated in Annex 1 of this Data Processing Agreement.

4.3 Notwithstanding EANV's consent within the meaning of the preceding paragraphs, the Data Processor will remain fully liable towards EANV for any consequences of subcontracting its activities to one or more Sub-Data Processors in accordance with Article 11.

4.4 EANV's consent pursuant to Article 4.1 is without prejudice to the fact that engagement of Sub-Data Processors in a country outside the European Economic Area without an appropriate level of protection also requires consent pursuant to Article 8.

4.5 The Data Processor will ensure that the Sub-Data Processor(s) is/are bound by the obligations of the Data Processor under this Data Processing Agreement, and will monitor compliance with these obligations.

5. Security

5.1 Without prejudice to the security standards the Parties agreed upon in the Main Agreement, the Data Processor will take appropriate technical and organisational measures to ensure the security of the processing of the Personal Data, listed in Annex 2. These measures at least include, without prejudice to the provisions of Article 28(3) and 32 of the GDPR, the following:

a. measures to ensure that the Personal Data can be accessed only by authorised personnel for the purposes set forth in Annex 1 of this Data Processing Agreement;
b. measures to protect the Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;
c. measures to identify imminent security breaches with regard to the processing of the Personal Data in the systems that are used to provide services to EANV;
d. the measures agreed upon by the Parties in Annex 2 of this Data Processing Agreement.

6. Audit requirements

6.1 The Data Processor will regularly check the security measures it has taken and in any case conduct a check at least once a year. At EANV's request, the Data Processor will demonstrate which measures it has taken in accordance with Article 5.1, will allow EANV to audit and test such measures and, based on the findings of these audits and tests, amend its security policy in accordance with EANV's further written instructions within the context of the applicable privacy legislation, including but not limited to Article 28(5) of the GDPR. Alternatively, EANV may use a statement by an independent external expert who gives an opinion on the measures taken by the Data Processor (Third Party Assurance).

6.2 The Data Processor will provide all reasonable cooperation in the relevant audits and tests, which must in any case be understood to include: providing access to buildings and data bases and making any relevant information available.

6.3 In the event that an audit and/or test shows that the Data Processor has failed to comply with its obligations under this Data Processing Agreement, the Data Processor will bear both its own costs and EANV's costs, incurred within the framework of the audit and/or the test, all this without prejudice to EANV's other statutory rights.

7. Security improvements

7.1 The Parties acknowledge that security requirements are subject to constant change, that an effective security system must be frequently evaluated and that regular improvements must be made to outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 5 on an on-going basis and will strengthen, supplement and improve these measures in accordance with Article 6.

7.2 EANV has the right to instruct the Data Processor to take additional security measures. The Data Processor will implement these additional security measures within a reasonable term (in principle:

within 4 weeks). Where an amendment to the Main Agreement is necessary in order to execute such an instruction, the Parties will agree upon an amendment to the Main Agreement.

8. Data transfers

8.1 The Data Processor will notify EANV without delay of any permanent or temporary planned or unplanned transfers of Personal Data to a country outside of the European Economic Area without an adequate level of protection (as referred to in Article 44 of the GDPR) and will only perform such a transfer (planned or otherwise) and will only perform such a planned or unplanned transfer after obtaining EANV's written consent. Annex 3 contains a list of countries outside the European Economic Area without an appropriate level of protection and the international organisations with regard to which EANV grants its consent to the Data Processor upon the conclusion of this Data Processing Agreement.

9. Information requirements and incident management

9.1 The Data Processor will promptly notify EANV – in any event within 24 hours after the Data Processor becoming aware thereof – of any privacy requests and incidents relating to the processing of the Personal Data. Data Processor will at all times cooperate with EANV upon its request and will follow EANV's written instructions in response to such privacy requests and/or with regard to such incidents, in order to enable EANV to perform a thorough investigation into the privacy request and/or incident, to formulate a correct response and to take suitable further steps in respect of the privacy request and/or incident. In addition, Article 11 of this Data Processing Agreement regarding liability and indemnity applies accordingly.

9.2 The term "privacy request" used in Article 9.1 must in any case be understood to mean: a compliant, a request for information or any other request concerning their rights as set out in the GDPR by a Data Subject or another natural person with regard to the processing of the Personal Data by the Data Processor.

9.3 The term "incident" used in Article 9.1 must in any case be understood to mean:

a. an investigation into or seizure of the Personal Data by government officials, or any indication that this is about to take place;

b. any unauthorised or accidental access, processing, deletion, loss or any form of unlawful processing of the Personal Data;

c. any breach of the security and/or confidentiality as set out in Articles 3 and 5 of this Data Processing Agreement that leads to the accidental or unlawful destruction, loss, alteration,

unauthorised disclosure of, or access to, the Personal Data, or any indication of such breach being imminent or having taken place.

9.4 The Data Processor will at all times have up-to-date and written procedures in place to enable it to provide an immediate response to EANV concerning an incident, and to cooperate effectively with EANV in handling the incident. The Data Processor will provide EANV with a copy of such procedures upon EANV's written request.

9.5 Any notifications pursuant to Article 9 will be addressed to EANV's IT Service Desk:

IT Servicedesk
Telephone: +31 (0) 88 - 0043010
Email: privacy@eindhovenairport.nl

The IT Service Desk can be contacted by telephone during office hours (Monday till Friday from 08.30 a.m. – 05.00 p.m.). If the call is not being answered, notification should be sent by email to privacy@eindhovenairport.nl with high priority.

A notification to the IT Service Desk must at least contain the following information:

- the start and end time, the start and end date and the location of the event;
- the nature and extent of the event;
- the department or part of the system involved in the event;
- the time required to determine the loss caused by the incident;
- the sort, the nature and extent of the Personal Data affected;
- the type and (estimated) number of Data Subjects that were affected;
- the expected consequences, including the consequences for the Data Subjects and a proposal for preventing loss and other negative consequences;
- the measures that have been or will be taken to mitigate the consequences of the incident; and
- the name and contact details of the Data Protection Officer or other contact person from whom additional information concerning the incident can be obtained.

9.6 The Data Processor is forbidden from, on its own initiative, informing Data Subjects who (may) have been affected by the incident and/or the competent authority, such as the Dutch Data Protection Authority of the incident.

10. Returning or destruction of Personal Data

10.1 Upon termination of this Data Processing Agreement, or upon EANV's written request, the Data Processor will, at EANV's discretion, either immediately destroy or return all Personal Data to EANV.

EANV can request Data Processor to provide a written confirmation of the destruction of Personal Data.

10.2 The Data Processor will notify all Sub-Data Processors and other third parties involved in the processing of the Personal Data of the termination of the Data Processing Agreement and will ensure that all such third parties will either destroy the Personal Data or return the Personal Data to EANV, at EANV's discretion.

11. Liability and indemnity

11.1 If either Party fails to comply with this Data Processing Agreement, that Party will be liable to compensate the other Party for the loss or damage it has suffered. 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.

11.2 In the event of intent or gross negligence on the part of the breaching Party, that Party will be liable for all loss or damage suffered or suffered in future by the other Party.

11.3 The Parties indemnify each other against any third-party claims in connection with a breach of the Data Processing Agreement. The aforementioned indemnity also includes any loss or damage and costs (including penalties) which the other Party suffers or incurs as a result of such a third-party claim.

11.4 Each Party is obliged to inform the other Party as soon as reasonably possible of an actual or a potential claim for liability or the actual or potential imposition of a penalty by the Supervisory Authority in connection with the Data Processing Agreement. Where reasonable, each Party is obliged to provide the other Party with information and/or assistance to enable it to conduct a defence against an actual or a potential claim for liability or a penalty. If a Party which has incurred costs in connection with the investigation of and conducting of a defence against actual or potential penalties of the Supervisory Authorities or third-party claims fails to inform the other Party in accordance with paragraph 4 of this Article, the other Party will not be liable for the costs.

12. Duration and termination

12.1 This Data Processing Agreement takes effect on the commencement date of the Main Agreement and ends automatically upon termination or expiry of the Main Agreement. In the event of extension of the Main Agreement, tacit or otherwise, this Data Processing Agreement will remain in force for the duration of the extension period.

12.2 Termination or expiry of this Data Processing Agreement will not discharge the Data Processor from its confidentiality obligations pursuant to Article 3 and obligations to return or delete the Personal Data pursuant to Article 10.

12.3 For the duration of the term of the Data Processing Agreement, EANV will be authorised to amend the terms, including but not limited to the technical and organisational measures to secure the processing of the Personal Data.

13. Miscellaneous

13.1 In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Agreement, the provisions of this Data Processing Agreement prevail.

13.2 This Data Processing Agreement contains the entire agreement between the Parties with regard to the processing of Personal Data as specified in Appendix 1 and takes the place of any previous oral and/or written agreements between the Parties within this framework.

13.3 In the case of transfers to countries outside the European Economic Area without an adequate level of protection and Data Processor performs such a (planned) transfer with EANV's written consent as provided in Appendix 3, than the provision in the Standard Contractual Clauses will prevail.

13.4 Any amendments to this Data Processing Agreement are valid only if agreed between the Parties in writing.

13.5 This Data Processing Agreement is governed by the laws of the Netherlands. Any disputes arising from or in connection with this Data Processing Agreement will be brought exclusively before the competent court in the district Oost-Brabant.

Thus agreed and signed,

on behalf of EANV

Name: R.A.J. Hellemons	Name: M.P.J. van den Bogaard .....
Title: Chief Executive Officer (CEO)	Title: Chief Operations Officer (COO) .....
Date:.....	Date: .....
Signature:	Signature:.....

on behalf of the Data Processor

Name:.....

Title: .....

Date:.....

Signature: .....

Annex 1

Overview of the categories of Personal Data, the purposes and other particulars on the basis of which the Data Processor will process the Personal Data:

To be completed by Data Processor (in consultation with EANV).

Personal Data category/categories	**Purpose(s)**	**Retention period(s)**
< Bijvoorbeeld: algemene (niet fiscale) personeelsgegevens in personeelsdossier>	< Bijvoorbeeld: in opdracht uitvoeren van salarisadministratie>	< Bijvoorbeeld: 2 jaar na uitdiensttreding medewerker>
< Bijvoorbeeld: naam, e-mail en inloggegevens van parkeerklanten EANV>	< Bijvoorbeeld: beheer softwaresysteem parkeeraccounts waarin deze gegevens voorkomen>	< Bijvoorbeeld: 1 jaar na laatste gebruik parkeeraccount>

To be completed by Data Processor

Sub- Data Processor(s): <yes/no>

If yes, please state the details of the Sub-Data Processor(s).

Name: <name>

Email: <email>

Telephone number: <telephone number>

Office address: <office address>

Located in: <country>

To be completed by Data Processor

Contact details of Data Processor's DPO/privacy officer:

Name: <name>

Email: <email>

Telephone number: <telephone number>

Office address: <office address>

Annex 2

1. **Managing information security risks**

   The Data Processor is responsible for managing all information security risks that may arise in the context of the performance of the Main Agreement and the processing of Personal Data by the Data Processor, its employees and any third parties it may engage (including subcontractors, suppliers and advisers). In this context, the Data Processor must proactively identify all information security risks, adopt and evaluate measures to mitigate these risks (the "**Security Measures**"). The Data Processor will, upon request from EANV, demonstrate that adequate Security Measures have been adopted.

2. **Training employees and third parties engaged by the Data Processor**

   The Data Processor will ensure that all employees involved in implementing the Main Agreement and the processing of Personal Data and any third parties it may engage have received the relevant information security training/awareness based on their roles and responsibilities in performing work under the Main Agreement and the processing of Personal Data. To comply with this obligation, the Data Processor will run a security awareness programme, together with education and training activities on a regular basis based on good practice. Also, the Data Processor will inform all employees and any third parties it may engage about the requirements that are set out in this annex.

3. **Audits and technical risk assessments**

   At least once a year, the Data Processor must perform an audit on EANV's service delivery infrastructure and systems or arrange for an independent third party to perform such a test at its own risk and expense. The Data Processor will implement corrective actions based on the findings of such audits and/or technical risk assessments, within the set timeframes. Data Processor will give EANV the opportunity to perform audits at any time desired by EANV, including, but not limited to, automated scans, PCI scans, etc. The Data Processor will, if EANV so requests, grant access to reports of audits and/or assessments that are less than two years old.

4. **(Personal) data security/encryption**

   The Data Processor applies cryptographic processing to protect the data (including personal data) it processes. Encryption must be applied when data is being transferred across public and/or from the internet-accessible networks and stored on fixed, portable devices or removable media such as USB sticks, and in other situations where data is vulnerable to unauthorised access (such as data that can

be accessed through the World Wide Web). Approved technology types include VPNs, SSH or HTTPS, or an equivalent technology for network security.

a. Secure technology such as Advanced Encryption Standard (EAS) technology with 256-bit keys or longer must be used for the storage of data. All keys used for this purpose must be managed in such a way that they are inaccessible to unauthorised persons and cannot be misused.

b. When using a website, the Data Processor must use HTTPS to make network traffic between the client and the web server unreadable by third parties if the data is sensitive or personal. The processor will give EANV the opportunity to perform audits at any time desired by EANV, including, but not limited to Qualys SSL server test with at least an A score.

c. The Data Processor will ensure that its website is protected by using an SSL/TLS certificate issued by a recognised public Certificate Authority (CA) such as Digicert, VeriSign, etc. The certificate must comply with the current requirements of the CA/Browser Forum Baseline Requirements for Contents of Publicly Trusted SSL/TLS Certificates. 'Self-signed certificates' are not permitted.

5. Password security

The Data Processor will ensure that passwords of all accounts, for both administrators and users, are stored with a secure one-way-hash mechanism (such as SHA-2 or SHA-3) with a "salt" addition.

6. Password rules

The Data Processor will ensure that the passwords for user accounts are strong (60 bit entropy), and contain at least the following complexity:

(i) at least 8 characters and made up of at least three of the following categories:

a. upper-case letters (A-Z),

b. lower-case letters (a-z),

c. figures (0-9),

d. special characters such as ! # $ ^ * - _ = ; : " ( ) { } [ ] | ` @ % & ? / \ +; or

(ii) at least 14 characters and made up of at least two of the following categories:

a. upper-case letters (A-Z),

b. lower-case letters (a-z),

c. figures (0-9),

d. special characters such as ! # $ ^ * - _ = ; : " ( ) { } [ ] | ` @ % & ? / \ +

These passwords must be changed at least once every 92 days. This requirement must be enforced through the IT service provided by the Data Processor.

Passwords for administrator accounts used by the Data Processor must be very strong, and must contain at least the following complexity: at least 15 characters and made up of at least three of the following categories:

a. upper-case letters (A-Z),
b. lower-case letters (a-z),
c. figures (0-9),
d. special characters such as ! # $ ^ * - _ = ; : ' " ( ) { } [ ] | ` @ % & ? / \ +

These password must be changed at least once every 180 days.

7. Multi-factor authentication

Multi-factor authentication technology must be used if the Data Processor's administrators require remote access via public networks, such as the Internet, to the systems on which personal or other data is processed or stored.

8. Patching and hardening

All known security patches released by the Other Party, developer or programmer have been applied to the software used by the Other Party (OS, database, and application software). Patches must be applied within 14 days of release for a base score of 7 or higher under the Common Vulnerability Scoring System (CVSS).

The Other Party ensures hardening of systems and software in accordance with CIS standards (or the security guidelines of the manufacturer) to ensure a safe configuration.

9. Account management

The Data Processor has formal procedures in place for creating, changing, and deleting accounts. In particular, it is important that accounts are deleted from the IT service in a timely manner. Any account that has not been used for 90 days must be disabled or deleted.

When an account is deleted, all related data must be irreparably erased unless the operation of the application will be disrupted. In that case the Data Processor must contact EANV's IT Service Desk (it@eindhovenairport.nl). These data must also be deleted from the backup. *Remark: it is allowed that data may exist in a back-up for maximal 35 days.*

10. Data minimization

The processor applies data minimization, which means that the processing of Personal Data is reduced to the utmost necessity.

11. Retention

The Data Processor will ensure that data is destroyed in a timely manner and in accordance with the agreed retention periods. In case of Personal Data or transactional data could also be done by anonymizing data. The method of anonymization must always be in consultation with EANV.

12. Procedures for handling information security incidents

The Data Processor has written procedures for promptly and effectively processing information security incidents and identified vulnerabilities in the security. The Data Processor had the obligations to immediately report to EANV any information security incidents detected and identified vulnerabilities in the security.

13. Audit IT system

When the IT system containing the Personal Data is delivered, EANV can carry out an audit or arrange to have an audit carried out to check whether the security of these IT resources had been set up in a technically correct manner and in accordance with the above requirements. The Data Processor must facilitate this audit. As an alternative, EANV may use a statement by an independent external expert who gives an opinion on the measures taken by the Data Processor (Third Party Assurance).

14. Erasing data and equipment

The Data Processor must erase any remaining personal or other data from any of its devices containing storage media, such as laptops or smartphones, before the devices are destroyed or reused. The personal or other data must be securely erased or, if the media cannot be securely wiped (such as an SSD), it must be securely destroyed.

Annex 3

Transmissions to countries outside of the European Economic Area without a suitable level of protection, and international organisations for which EANV has granted its consent:

☒ Not applicable

☐ Applicable:

Country/countries:

<land(en) buiten de Europese Economische Ruimte zonder een passend beschermingsniveau>

International organisations:

<naam internationale organisatie(s) + land>

Parties agree, for the purpose of legal transfers, the following Standard Contractual Clauses.