

DATA PROCESSING AGREEMENT belonging to <>

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), **< name >**, and its Chief Operations Officer (COO), Mrs. 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 concluded one or more agreements with Data Processor for the provision of various services by Data Processor to EANV, or will conclude such an agreement. These agreements are hereinafter referred to as the **“Main Agreement”** and are further specified in the title of this data processing agreement.
- II. During the performance of the Main Agreement, Data Processor will process data of 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. Having regard to 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 “**Data Processing Agreement**”) applies solely to the processing of personal data within the scope of the Main Agreement between the Parties.
- 1.2 Terms such as “Processing”, “Personal data”, “Data Controller”, “Data Processor”, “Data Subject” and the “Party Concerned” have the meaning ascribed to them in the GDPR.
- 1.3 It is possible that the Data Processor will process personal data (hereinafter to be referred to as the “**Personal Data**”) on behalf of EANV in the course of the performance of the Main Agreement with EANV. An overview of the categories of Personal Data and purposes for which the Personal Data are being processed is provided in Appendix 1.

2. The Data Controller and the Data Processor

- 2.1 The Data Processor will act as the Data Processor and EANV will act as the Data Controller.
- 2.2 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.
- 2.3 If the Data Processor determines the purposes and the means of processing in contraventions of the GDPR and this Data Protection Agreement, Data Processor will be regarded as the Data Controller (for that part of the processing).
- 2.4 More specifically, EANV may give instructions with regard to the retention period of all the Personal Data referred to in Appendix 1.
- 2.5 The Parties conclude the Main Agreement in order to take advantage of the expertise of the Data Processor in the context of the Main Agreement and the processing of Personal Data for the purposes set out in Appendix 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 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. The Data Processor will ensure that all such persons and parties have signed an adequate Sub-Data Processors Agreement to that end as further specified in Article 8. The Data Processor will, at the request of EANV, provide EANV with copies of this/these agreement(s).

3.2 The Parties will treat all information the Data Processor is required to provide to EANV by virtue of Article 4 of this Data Processing Agreement as strictly confidential.

4. Security

4.1. Without prejudice to the security standards agreed upon in the Main Agreement by the Parties, the Data Processor will take appropriate technical and organisational measures to ensure the security of the processing of the Personal Data, listed in Appendix 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 Appendix 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 of the Personal Data;
- c. measures to identify security breaches – imminent or not – with regard to the processing of Personal Data in the systems that are used to provide services to EANV;
- d. the measures agreed upon by the Parties in Appendix 2 of this Data Processing Agreement.

4.2. 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 the request of EANV, the Data Processor will demonstrate which measures it has taken in accordance with Article 4.1, allow EANV to audit and test such measures and, as a result of 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. As an alternative, EANV may use a statement by an independent external expert who will give an opinion on the measures taken by the Data Processor (Third-Party Assurance).

5. Improvements to Security

5.1. The Parties acknowledge that security requirements are subject to constantly 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 4 on an on-going basis and will tighten, supplement and improve these measures in order to ensure compliance with the requirements set out in Article 4.

- 5.2. EANV has the right to instruct the Data Processor to take additional security measures. 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.

6. Data Transfers

- 6.1. The Data Processor will immediately notify EANV of any permanent or temporary transfers of Personal Data (planned or otherwise) 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) after obtaining EANV's written consent. Appendix 3 contains a list of countries without an appropriate level of protection for which EANV grants its consent to the Data Processor upon the conclusion of this Data Processing Agreement.

7. Information Obligations and Incident Management

- 7.1 The Data Processor will at all times immediately – at least within 24 hours after the Data Processor has become aware of it – notify EANV of any privacy requests and incident 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 10 of this Data Processing Agreement regarding liability and indemnity accordingly applies.
- 7.2 The term “privacy request” used in Article 7.1 is in any case taken to mean: a compliant or request (for information) or any other request concerning his rights pursuant to the GDPR by a Data Subject or another natural person with regard to the processing of the Personal Data by the Data Processor.
- 7.3 The term “incident” used in Article 7.1 is in any case taken 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 4 of this Data Processing Agreement leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or that it is about to take place.

7.4 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.

7.5 Any notifications pursuant to Article 7 will be addressed to EANV's ICT Service Desk:

ICT Servicedesk

Tel: +31 (0) 88 - 0043010

e-mail: privacy@eindhovenairport.nl

The ICT 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 e-mail to privacy@eindhovenairport.nl with high priority.

A notification to the ICT Service Desk must contain at least 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 where the event occurred;
- the time required to determine the damage caused by the incident;
- the nature and extent of the affected Personal Data;
- type and (estimate of) number of affected persons involved;
- the expected consequences, including the consequences for those involved and a proposal to prevent damage and other negative consequences;
- measures taken and to be taken to mitigate the consequences of the incident; and
- the name and contact details of the data protection officer or other contact person, where additional information concerning the incident can be obtained.

7.6 The Data Processor is not allowed, on its own initiative, to inform those who are (possibly) affected by the incident and/or the competent authority, for example the Dutch Data Protection Authority/*Autoriteit Persoonsgegevens*, of the incident.

8. Engagement of Sub-Data Processors

- 8.1 The Data Processor will not subcontract any of its activities consisting, in part or in full, of the processing of the Personal Data to one or more Sub-Data Processors without the prior written consent of EANV.
- 8.2 Notwithstanding the consent of EANV within the meaning of the preceding paragraph, the Data Processor will remain fully liable vis-à-vis EANV for any consequences of subcontracting with one or more Sub-Data Processors in accordance with Article 10.
- 8.3 EANV's consent pursuant to Article 8.1 will not alter the fact that consent is also required under Article 6 for the engagement of Sub-Data Processors and their possible third parties (including international organisations) in a country outside the European Economic Area without a suitable level of protection.
- 8.4 The Data Processor will ensure that the Sub-Data Processor and possible third parties engaged by the Sub-Data Processor are bound by the obligations of the Data Processor under this Data Processing Agreement, and will ensure compliance therewith.

9. Returning or Destruction of Personal Data

- 9.1 Upon termination of this Data Processing Agreement, or upon EANV's written request, the Data Processor will, at the discretion of EANV, 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.
- 9.2 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 the discretion of EANV.

10. Liability and Indemnity

- 10.1 The Parties indemnify each other and hold each other harmless against all claims, actions and third-party claims for losses, damage, fines and expenses incurred by the other Party and arising directly or indirectly from or in connection with a breach of this Data Processing Agreement by a Party.
- 10.2 EANV does not indemnify the Data Processor against losses, damage, fines or expenses incurred by the Data Processor and arising directly or indirectly from or in connection with the processing of Personal Data by the Data Processor which is not in compliance with EANV's lawful instructions.

11. Duration and Termination

- 11.1 This Data Processing Agreement will take effect on the commencement date of the Main Agreement and ends automatically when the Main Agreement is terminated or expires. 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. Is this Data Processing Agreement is still valid after a period of three (3) years, EANV is authorized to re-assess and adjust the conditions, including but not limited to, the technical and organizational measures to secure the processing of the Personal Data.
- 11.2 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 9.

12. Miscellaneous

- 12.1 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.
- 12.2 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 replaces any previous oral and / or written agreements between the Parties in this context.
- 12.3 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.
- 12.4 Amendments to this Data Processing Agreement are only valid if agreed between the Parties in writing.
- 12.5 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.

For EANV

Name: < name > Name: Mrs. M.P.J. van den Bogaard

Title: Chief Executive Officer (CEO) Title: Chief Operations Officer (COO)

Date: Date:

Signature: Signature:.....

For the Data Processor

Name:

Title:.....

Date:

Signature:

Appendix 1

Overview of the categories of Personal Data and purposes for which the Personal Data are being processed.

Category: **< categories >**

Purpose: **< purposes >**

Retention period: **< retention period >**

Sub-Processors: **< yes/no >** *If yes, please provide us with the details of the sub processors and a copy of the data processing agreement which has been agreed upon between your organization and the sub processor.*

Contact details of Data Processor's DPO/privacy officer: **< name/ e-mail/ telephone number/ office address >**

Appendix 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.

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 ICT 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 to the systems on which personal or other data is processed or stored.

8. Patching

All known security patches released by the Data Processor, developer or programmer have been applied to the software used by the Data Processor (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).

9. Account management

The Data Processor has formal procedures in place for creating, changing and deleting administrator accounts. In particular, it is important that accounts are deleted from the ICT 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 ICT Service Desk (ict@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.

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.

Appendix 3

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

☒ Not applicable

☐ Applicable

Country/countries:

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