DATA PROCESSING AGREEMENT

This Data Processors Agreement (hereinafter: DPA) is an integral part of the Terms of Services of iotspot B.V., located at Veemarktkade 8, 5222 AE in 's-Hertogenbosch, The Netherlands and registered with the Chamber of Commerce under number 65535294, (hereinafter: iotspot, we, us or our) and applies to all forms of processing of personal data that we perform while using iotspot 'Smart Workspace Platform Services' (hereinafter: Services) by a party that procures these Services (hereinafter: Customer, you or your).

1. Data processing

1.1. This DPA applies to your use of our Services and the related processing and storage of your data in our mobile applications, online Cloud services and related backups, plus those purposes that are reasonably related thereto or that are determined with further consent of both parties. In this context, iotspot is the "Processor" and the Customer is the "Processing Responsible Party", as both terms are defined in the General Data Protection Regulation (hereinafter: GDPR) respectively.

1.2. Our Services offer Customers and those involved a number of control measures, including privacy protection functionality, that you can use to modify, delete or limit customer data. You may use these as technical or organizational measures to comply with your obligations as "Processing Responsible Party" under laws and regulations such as the GDPR.

1.3. The personal data processed by us in the context of the activities referred to in paragraph 1 and the categories of the data subjects from whom they originate are included in Appendix 1. We will not process the personal data for any other purpose than as mentioned in this DPA.

1.4. You and iotspot agree that this DPA, as part of our Terms of Service, are your - in accordance with the GDPR - documented data processing instructions.

1.5 The personal data to be processed on behalf of the Customer, thus remain the property of you and/or the persons concerned.

2. Obligations of iotspot

2.1. With regard to the processing operations referred to in Article 1, you and we will ensure compliance with the applicable laws and regulations, including in any case the laws and regulations in the field of the protection of personal data, such as the GDPR.

2.2. iotspot will inform Customer, at its first request to that effect, about the measures taken by us regarding our obligations under this DPA.

2.3. The obligations of iotspot arising from this DPA also apply to those who process personal data under our authority, including but not limited to employees, in the broadest sense of the word.

2.4. We will inform you immediately if we believe that any instruction given by you is contrary to the legislation referred to in paragraph 1.

2.5. iotspot will, to the extent within our control or if required by law, assist Customer in carrying out data protection impact assessments (PIAs). We may charge you a reasonable fee for our activities in this regard.

3. Transfer of personal data

3.1. We process personal data in countries as determined by the then applicable laws and regulations of your country of residence. Transfers to countries outside the scope of the then current legal provisions are permitted, whereby we will comply with the then applicable legal requirements for such a transfer.

3.2. iotspot will inform you about the country or countries that is/are concerned.

4. Division of responsibility

4.1. iotspot will only process your customer data in the context of your use of our Services.

4.2. iotspot is solely accountable for the processing of the personal data under this DPA, in accordance with our Terms of Service and under the express (final) accountability of you. We are explicitly not accountable for any other processing of personal data, including in any case, but not limited to, the

collection of personal data by the Customer, processing for purposes not reported by you to us, processing by third parties and/or for other purposes.

4.3. You guarantee that the content, the use and the assignment for the processing of personal data as referred to in this DPA are not unlawful and do not infringe on any right of third parties.

5. Engagement of third parties or subcontractors

5.1. You allow us to use the online Cloud services of authorized third parties within the framework of Amazon Web Services Inc. (AWS), where Database and Webserver services are purchased. The data processing agreement between us and AWS is in accordance with the then current GDPR and can be read at the following URL: (https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf);

5.2. iotspot guarantees the correct fulfilment of the obligations from this DPA by the authorized third parties under paragraph 1 and in the event of errors of these third parties is liable for all damage as if it had committed the error(s) itself.

5.3. You allow us, after explicit and written approval by you, to consider and treat as a "Processor" of your personal data, within the framework of this DPA, third parties that you have engaged in relation to our Services in any capacity whatsoever. You accept full responsibility, as we do not accept any responsibility, for the correct observance of the obligations from this RFO by this third party designated by you.

6. Data protection and information security

6.1. We will make every effort to take appropriate technical and organizational measures against loss or against any form of unlawful processing (such as unauthorized access, infringement, alteration, or disclosure of personal data) regarding the processing of your personal data.

6.2. iotspot has - in accordance with our Information Security Statement (https://iotspot.zendesk.com/hc/en-nl/articles/360016417399-Information-security) - taken at least the following measures:

a) Logical access control, using strong passwords, personal programmable keys;

b) Physical measures for access security;

c) Encryption of digital files containing personal data;

d) Sample checking of compliance with the policy;

e) Security of network connections via Secure Socket Layer (SSL) technology;

f) Purpose-Bound Access Restrictions; and

g) Control of issued authorizations.

6.3. iotspot does not guarantee that the security is effective under all circumstances. If there is no explicitly described security in this DPA, we will make every effort to ensure that the security meets a level that is not unreasonable in view of the state of the art, the sensitivity of the personal data and the costs associated with fitting the security.

6.4. You only make personal data available to us for processing if you have assured yourself that the required security measures have been taken. You are responsible for compliance with the measures agreed between you and us.

7. Duty to report

7.1. Customer is at all times responsible for reporting a data breach (which means: a breach of security that accidentally or unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of or access to transmitted, stored or otherwise processed data; unless it is unlikely that the breach in connection with personal data poses a risk to the rights and freedoms of natural persons) to supervisor and/or data subjects.
To enable you to comply with this legal obligation, iotspot will notify you of the security breach and/or data breach within 48 hours of the leak becoming known to us.

7.2. The duty to report in any case includes reporting the fact that there has been a data breach. In addition, the following must be reported:

a) The nature of the personal data breach, indicating where possible the categories of data subjects and personal data registers involved and, approximately, the number of data subjects and

personal data registers involved;

b) The name and contact details of the Data Protection Officer or any other contact point from which further information may be obtained;

c) The likely impact of the personal data breach;

d) The measures proposed or taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate any adverse consequences thereof.

8. Handling data subject requests

The Services offer the opportunity for you as a person involved to exercise your legal rights. In the event that you as a data subject submits a request to us to exercise his/her legal rights, we will process the request, provided it is within the boundaries of our Terms of Service. In the event that the request falls outside the scope of the Terms of Service, iotspot will forward the request to you and you will process the request further. We may inform the person concerned about this course of events.

9. Return or deletion of customer data

The Services offer you and those involved the opportunity to request or remove customer and personal data. Until the termination date of any agreement between you and us regarding our Services, this option will continue to apply to you and those concerned. After termination, we will remove the customer and personal data from the ICT applications on which our Services are based immediately but no later than 14 days after the termination date, with the exception of the data that the person(s) concerned have stored within our mobile application and remains stored there because the person concerned does not remove our mobile application from the mobile phone in question.

10. Non-disclosure and confidentiality

10.1. All personal data that iotspot receives from the Customer and/or collects itself within the framework of this DPA are subject to non-disclosure and confidentiality towards third parties. We will not use this information for any other purpose than for which we have obtained it.

10.2. This confidentiality obligation does not apply if you have given explicit permission in writing to provide the data to third parties, if the provision of the data to third parties is logically necessary in view of the nature of the assignment and the execution of this DPA, or if there is a legal obligation to provide the data to a third party.

11. Audit

11.1. In case of concrete suspicion of abuse and/or concrete suspicion of insufficient compliance with the security measures, Customer has the right to execute audits by an independent expert third party, who is bound to confidentiality, to check compliance with the security requirements, compliance with the general rules concerning the processing of personal data, misuse of personal data by our employees, compliance with all points of this DPA, and everything that is directly related to this.

11.2 You shall give ten working days' notice of an audit and the audit must not unduly disrupt our business operations.

11.3. We will cooperate with the audit and provide all information reasonably relevant to the audit, including supporting data such as, but not limited to, application or system log files, and employees as timely as possible.

11.4. The findings of the audit will be assessed by you and us in mutual consultation and if deemed necessary implemented accordingly by one or both of the parties.

11.5. The costs of the audit shall be borne by Customer.

12. Liability

You accept and expressly agree with us that our Terms of Service apply with regard to liability.

13. Term and termination

13.1. This DPA is established between parties by:

a) Use of our Services by you and/or those involved, which use starts by an unambiguous 'Opt-in' by you or those involved at the first use of our Service; or

b) Signing this DPA by both parties with the date of the last signature as the starting date.

13.2. This DPA has been entered into for the duration as stipulated in the main agreement between you and us and in the absence thereof at least for the duration of your use of our Services.

14. Legal provisions and dispute resolution

14.1. This DPA and its implementation are governed by Dutch law.

14.2. If a competent court determines that a provision of this DPA is invalid, then that provision will be removed from this IMP without affecting the validity of the rest of this DPA. The remaining provisions remain in force and enforceable.

14.3. In case of a conflict between our then current Terms of Service and this DPA, the provisions of this DPA prevail.

14.4. Any dispute arising from or related to this DPA, which is not amicably settled, will be submitted to the competent court of the district in which iotspot is established.

Agreed and signed in duplicate,

Customer,	iotspot B.V.
Date:	19 May 2021
Name:	Name: Marnix Lankhorst
Function:	Function: Managing Director
(Authorised signatory)	

ANNEX 1: SPECIFICATION OF PERSONAL DATA AND DATA SUBJECTS

A. Personal data

The table below defines the personal data that we process within our Services. For each record, a definition is given, specifying whether it is mandatory or at the choice of the data subject and the period for which the relevant information is identifiable within our Service.

#	Definition of record	Mandatory or By choice	Identifiable period
1	Name, as entered by the data subject	Mandatory	Until the data subject terminates the account or the Customer requests data deletion and this has been carried out by us.
2	E-mail address of the Customer's e-mail domain as entered by the data subject.	Mandatory	Until the data subject terminates the account or the Customer requests data deletion and this has been carried out by us.
3	Profile picture, as the data subject wishes to enter.	By choice of the data subject; not mandatory	Until the data subject terminates the account or the Customer requests data deletion and this has been carried out by us.
4	Telephone number, as the data subject wishes to enter.	By choice of the data subject; not mandatory	Until the data subject terminates the account or the Customer requests data deletion and this has been carried out by us.
5	LinkedIn URL, as the data subject wishes to enter.	By choice of the data subject; not mandatory	Until the data subject terminates the account or the Customer requests data deletion and this has been carried out by us.
6	Department, as the data subject wishes to enter.	By choice of the data subject; not mandatory	Until the data subject terminates the account or the Customer requests data deletion and this has been carried out by us.
7	Role, as the data subject wishes to enter.	By choice of the data subject; not mandatory	Until the data subject terminates the account or the Customer requests data deletion and this has been carried out by us.
8	I am an Emergency Rescue Officer (Yes/No) as the data subject wishes to enter.	By choice of the data subject; not mandatory	Until the data subject terminates the account or the Customer requests data deletion and this has been carried out by us.
9	Indirect: If the data subject makes a reservation for a workplace, the possible location of the data subject can be derived from the office location where the workplace can be reserved.	By choice of the data subject; not mandatory	From the time of reservation until the end of the 24 hours of the reservation date.

B. Data subject categories

Depending on the definition of authorization of the Customer and those concerned, we process the aforementioned personal data for the categories of concerned parties listed below:

a) Customers, annex Account holders;

b) Personnel (of the Customer);

c) Suppliers (of the Customer);

d) Prospective customers(of the Customer);

e) Tenants (of the Customer); and

f) Visitors (of the Customer).