Data Processing Agreement – Kooi Trading B.V.

Kooi Trading B.V., hereinafter referred to as "**Processor**", registered and operating under existing Dutch laws with business address at Zonnedauw 10, 9202 PA, The Netherlands, processes personal data for _____, hereinafter referred to as "**Data Controller**", within the parameters of the provision of Article 4 paragraph 2 and Article 28 of the GDPR (General Data Protection Regulation) based on the main agreement. Regarding the data protection obligations, the following provisions, hereinafter the "**Processing Agreement**", apply:

Considering that:

A. The parties have entered into an agreement with regard to services provided by Kooi Trading B.V. hereinafter referred to as the "**Main Agreement**";
B. The Processor has access to Personal Data, within the meaning of the General Data Protection Regulation (GDPR), of the Data Controller and/or of customers van de Data Controller (hereinafter referred to as "Personal Data"), within the meaning of the General Data Protection Regulation (GDPR), whether with the directive to process this Personal Data or not;
C. The parties agree, with regard to the processing of the Personal Data, to observe the provisions of this Data Processing Agreement;
D. The Processor will comply with national and international laws and regulations as well as the provisions of this Data Processing Agreement when accessing Personal Data.

1. Definition of Terms

1.1. **Data Subject**: the person to whom a Personal Data relates.
1.2. **Processor**: the person who processes Personal Data on behalf of the Data Controller without being subject to his direct authority.
1.3. **Data breach**: a breach of the security of Personal Data that has adverse consequences for the protection of personal data.
1.4. **Personnel**: the persons to be engaged by the Parties for the implementation of this Data Processing Agreement, who will work under their responsibility.
1.5. **Personal Data**: any data concerning an identified or identifiable natural person. A person is considered identifiable when they can be directly or indirectly identified, for example, by reference to a name, identification number, location data, online identifier, or other factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.
1.6. **Sub-processor**: third party engaged by the Processor to process Personal Data on behalf of the Processor without being subject to the direct authority of the Processor. In the case of the services provided by Kooi Trading B.V. is this in any case Kooi Service & Security Center B.V. with its registered office and principal place of business at Zonnedauw 10, 9202 PA, Drachten.

1.7. **Data Controller**: The Controller for Data Processing within the meaning of the GDPR. If the Data Controller processes Personal Data on behalf of a customer, the customer functions as the Data Controller in this Processing Agreement.

1.8. **Processing**: Any act or set of acts related to Personal Data, including in any case the collection, recording, organization, storage, updating, modification, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of making available, bringing together, associating, as well as blocking, exchanging or destroying data.

1.9. **Main Agreement:** Agreement in which the services provided by Kooi Trading B.V. is stated in detail, in particular what type of service and duration of service.

2. Subject, Purpose, & Retention Period

2.1. If the Processor has committed itself in the Main Agreement to process Personal Data, Processor will do so with great care and in accordance with the purposes of the processing and thereby both national and international laws and regulations with regard to Personal Data, in particular the regulations from the GDPR regulation, and observe the provisions of this Data Processing Agreement; if and insofar as the Data Controller has informed the Processor in good time in advance of the availability of the Personal Data and the location where these Personal Data are stored.

2.2. The purpose of the data processing by the Processor is the execution of the Main Agreement and the provision of the services agreed therein by Kooi Trading B.V. on behalf of the Data Controller.
The processing specifically includes the detection and transmission of signals relating to abnormal or undesired situations at the Data Controller's locations, such as (suspected) unauthorized presence or other potentially hazardous events. These signals are generated within the technical capabilities of the deployed surveillance system and transmitted to the Control Room. The Control Room processes these signals solely for the purpose of monitoring, analyzing, and identifying such events.

2.3. The processing of the personal data under this Data Processing Agreement relates to:

- (unauthorized) data subjects who may be recognizable on video images;
- Contact and company details of the Data Controller (including, but not limited to the name, address, telephone number, e-mail address, Chamber of Commerce registration number, and bank account information).

2.4. The retention periods for Personal Data are established in accordance with applicable laws and regulations and aligned with the purposes of the Processing. For camera footage, the following retention periods apply:

- **Regular recordings:** footage routinely captured by the Processor's camera systems is retained for a maximum period of 7 days;
- **Alarm recordings:** footage recorded in response to an alarm trigger or incident report is retained for a maximum period of 28 days.

Longer retention periods are only permitted if legally required or necessary to protect the legitimate interests of the Data Controller, for example in the context of an incident investigation.
The established retention periods are documented internally, periodically reviewed and adjusted if necessary, and can be made available to the Data Controller upon written request.

3. Obligations of the Data Controller

3.1. The Data Controller guarantees that it complies with all regulations from the GDPR. The controller has taken the necessary security measures.

3.2. The Data Controller will notify the Processor of changes to the Processing (if applicable) and any consequences thereof in a timely manner, in principle, within 10 working days.

3.3. The Data Controller guarantees that its personnel comply with the provisions of the GDPR Regulations and the provisions of this Data Processing Agreement, if and insofar as they are involved in any way in the Processing of Personal Data.

3.4. The Data Controller guarantees that the assignment to Process the Personal Data (if applicable) is not unlawful and does not infringe the rights of third parties.

3.5. The Data Controller gives the Processor permission to engage third parties for the Processing in the context of the implementation of the Main Agreement and this Processor Agreement.

4. Obligations of the Processor

4.1. The Processor will only view and/or process the Personal Data if and insofar as this is necessary for the execution of the Main Agreement and will follow all reasonable instructions from the Data Controller.

4.2. The Processor will not store the Personal Data in a location outside the European Economic Area or transfer it to countries outside the European Economic Area, without the prior written consent of the Data Controller. The Data Controller can attach conditions to its consent.

4.3. The Processor guarantees that its Personnel is aware of the requirements set by the GDPR Regulation and that it complies with the provisions of the GDPR Regulation and the provisions of this Data Processing Agreement, if and insofar as they are involved in any way in the Processing of Personal Data. Processor's employees are bound by a duty of confidentiality.

4.4. At the first request of the Data Controller, the Processor will immediately hand over to the Data Controller or destroy all copies of the Personal Data that originated from and/or are in assignment under the direction of the Data Controller.

Obligations with regard to Processing

The articles 4.5 t/m 4.7 only apply if the Processor has committed itself to Processing.

4.5 Processor will take appropriate technical and organizational security measures to protect the Personal Data against loss and unlawful processing. Considering the technology being used and the costs of its implementation, these measures guarantee an appropriate level of security in view of the risks involved in the processing and the nature of the data to be protected.

4.6 The Processor grants the Data Controller its full and timely cooperation to allow Data Subjects to access their personal data, to have their personal data removed or corrected, and/or to demonstrate that these personal data have been removed or corrected or, if the Data Controller disputes the Data Subject, to record that the Data Subject considers his Personal Data to be incorrect.

4.7 The Processor takes adequate internal control measures to comply with the obligations under this Data Processing Agreement and records them in a way that makes it easy to monitor compliance. When Processing Personal Data, activities and incidents related to the Personal Data are recorded in log files.

4.8 At the request of the Data Controller, the Processor will cooperate with the encryption when transporting confidential information over networks. If this leads to higher costs for the processor, the Data Controller will reimburse these costs.

4.9 The Data Controller can have the Processing of Personal Data checked once a year for correct compliance with the Data Processing Agreement by means of an investigation by an independent registered EDP (Electronic Data Processing) Auditor. The Auditor will be bound to secrecy. The Processor will provide all information requested by the Auditor. All costs of the investigation will be borne by the Data Controller.

4.10 The content and scope of the assignment for Processing and costs thereof are in accordance with what has been agreed in the Main Agreement. The Processor will follow instructions from the Data Controller regarding the processing and/or storage of Personal Data.

5. Sub-processor

5.1. The Processor may outsource the performance of the Data Processing Agreement in whole or in part to a Sub-processor, after prior written consent from the Data Controller. The Data Controller will not, within good reason, withhold permission. The Processor always remains the point of contact for the Data Controller and is responsible for the compliance of the provisions of this Data Processing Agreement.

5.2. The Processor will impose the same obligations on the Sub-processor arising from this Data Processing Agreement and monitor compliance of the same by the Sub-processor.

5.3. The Processor is fully liable to the Data Controller for the consequences of outsourcing work to a Sub-processor.

5.4. Article 4.2 also applies in full to the Sub-processor.

5.5. The Processor currently performs the Main Agreement in cooperation with the Sub-processors listed in **Appendix 1**, to which the Data Controller agrees.

6. Provision of Personal Data

6.1. The Processor is not permitted to provide Personal Data to anyone other than the Controller, unless on the basis of a legal obligation or with written permission from the Data Controller. The Processor will confirm every provision to a third party in writing, stating all parties and/or persons involved.

6.2. If the Processor provides Personal Data to the Data Controller, whether on request or not, the Data Controller will never publish or distribute the Personal Data provided without a court order and it will never harm the honor and reputation of the Processor. Either Processor or Data Controller may be required to disclose Personal Data to competent authorities under applicable national laws, without a court order, depending on the jurisdiction.
In the event of a violation to this article, the Data Controller will pay a fine of €10.000 per incident per day to the Processor.

6.3. If the Processor is required to provide Personal Data on the basis of a legal obligation, the Processor will:

- Verify the basis of the request and the identity of the person who requested it and, prior to the provision, inform the Data Controller;
- Limit the provision to what is legally required;
- Enable the Data Controller to exercise the rights:
    - Of the Data Controller and the Data Subjects, and;
    - To defend the interests of the Data Controller and the Data Subjects.

7. Data Security

7.1. The Data Controller and the Processor will secure the Personal Data and, if applicable, the Processing thereof in accordance with the regulations set out in the GDPR, and in other (special) legislation and European rules and guidelines. The level of security should be in accordance with common standards such as ISO27001.

7.2. The Data Controller and the Processor will make every effort to secure the Personal Data and to keep it secured against intruders and against external disasters as well as careless, incompetent or unauthorized use. Both parties take measures to guarantee security. These measures include, but are not limited to, access security, physical security, cryptography and continuity management.

7.3. If the Data Controller requests this in writing, the Processor will take special measures for the security and/or secrecy thereof with regard to the Personal Data indicated therein. If this leads to higher costs for Processor, Controller will reimburse these costs.

8. Data Leaks

8.1. In the event that either the Data Controller or the Processor becomes aware of a (suspected) personal data breach that may also be relevant to the other Party, the respective Party shall notify the other without undue delay, and in any case no later than within twenty-four hours of discovery, by means of a written notice. Such notice shall include, at a minimum:

- description of the nature of the personal data breach, including the categories of data subjects and personal data concerned;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken to address the personal data breach and mitigate its adverse effects;
- the contact details of a designated point of contact for obtaining further information.

8.2. In accordance with the GDPR, there is a Data Breach Notification Obligation. This means that organizations must report a serious data breach to the competent supervisory authority within 72 hours. The Processor and the Data Controller shall comply with this notification obligation and, if necessary, make additional agreements regarding the manner of fulfilling this obligation, as well as the detection, identification, and investigation of security incidents and their causes. Notification to the supervisory authority shall be made to the authority competent in the jurisdiction of the Data Controller.

9. Confidentiality

9.1. All the data belonging to the Data Controller and its customers are confidential and will be treated as such by the Processor. The Processor is obliged to maintain the confidentiality of all Personal Data and information that it processes, or of which in the context of the Main Agreement or this Data Processing Agreement is made aware.

9.2. The confidentiality does not apply to the following information:

- Information which is publicly known without the disclosure of which being a result of an unauthorized act;
- Disclosure of which is required by a statutory provision or court order, subject to prior written notice from the disclosing party to the party whose information it concerns;
- Which a Party has independently developed;
- Which a Party already possesses without any obligation of confidentiality.

10. Intellectual Property

10.1. All intellectual property rights, including copyrights, database rights and all other intellectual property rights as well as similar rights to protect information on the collection of data and Personal Data, copies or adaptations thereof, rests with the Data Controller (or a customer of the Data Controller).

10.2. All intellectual property rights - including copyrights, database rights and all other intellectual property rights as well as similar rights to protect information - on the products and services of the Processor are vested in the Processor.

11. Liability and Insurance

11.1. Insofar as the Processor is liable for damage under this Data Processing Agreement, the Processor's total liability is limited to compensation for direct damage, and this to a maximum of the amount of the compensation paid for the use of the service or product in the last 6 months prior to the occurrence of the damage.

11.2. The Processor does not carry any liability for indirect damage. Indirect damage includes consequential damage, lost profit, lost savings, reduced goodwill, damage due to business interruption, and damage as a result of claims for third parties.

12. Duration and Termination

12.1. The Data Processing Agreement enters into force on the same day that the Main Agreement is signed by the Parties.

12.2. The provisions on duration and termination of the Main Agreement apply as provisions on duration and termination for the Data Processing Agreement. When the Main Agreement is terminated or ended for whatever reason, the Data Processing Agreement is also terminated or ended.

12.3. In the event of the termination of the Data Processing Agreement, the Processor will, at the Data Controller's discretion, destroy all Personal Data belonging to the Data Controller.

12.4. Obligations that by their nature are intended to continue after the termination of the Data Processing Agreement will continue to apply after termination. These obligations include the provisions on confidentiality, transfer and destruction, liability and applicable law.

13. Dissolution

13.1. Each Party may dissolve the Main Agreement in whole or in part if the other party imputably fails to comply with the Data Processing Agreement and the shortcoming has not been remedied even after notice thereof, without prejudice to the right to compensation.

13.2. Each Party may dissolve the Main Agreement in whole or in part with immediate effect without notice thereof if the other party is granted a moratorium, if bankruptcy is filed with regard to the other party, if the company of the other party is liquidated or terminated other than for the purpose of reconstruction or amalgamation of companies.

14. Supplemental Provisions

14.1. Amendments to this Data Processing Agreement or additions hereto are agreed in writing between the Processor and the Data Controller. Changes or additions will be recorded in an addendum to this agreement and will only be binding if this addendum is signed by both Parties.

14.2. Any disputes arising from this Data Processing Agreement, after an attempt to resolve the dispute by mutual agreement has proved fruitless, will be settled by arbitration in accordance with the rules and procedures of the Netherlands Arbitration Institute, whereby the arbitrator(s) will apply Dutch law.

On behalf of Kooi Trading B.V.	On behalf of:
Name:	Name:
Function:	Function:
Date :	Date :
Signature :	Signature :

Appendix 1 List of Sub-processors

The Processor currently cooperates with the following sub-processors in the execution of the Main Agreement, with which the Data Controller agrees.

- **Kooi Service & Security Centre B.V. (Nederland):**
  Monitoring and Alarm Receiving Centre: processing the video images.
  Zonnedauw 10, 9202 PA, Drachten.