PROTECTION OF PRIVACY AND TRANSPARENCY OF THE STATE Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 PRECAUTIONS-WARNING in personal data protection matter no. 2.1.-6/21/23 Preceptor of the Data Protection Inspector Raiko Kaur Time and place of precept 02.09.2021, Tallinn Addressees of precept Pallimehed OÜ (11413171) pallimehed@hot.ee marko@peetripizza.ee Persons responsible for the addressees Member of the Management Board RESOLUTION: § 56 (1) (2) 8) of the Personal Data Protection Act , § 58 (1) and Article 58 (1) (d) and (2) (e) and (f) of the General Regulation on the Protection of Personal Data (IKÜM), as well as taking into account Articles 5, 6, 12, 13 and 34 of the IKÜM, 1. Pallimehed OÜ must either: 1.1. discontinue the use of cameras, which may be in the line of sight of employees, or (see paragraphs 1 and 2 of the Inspectorate's recitals, including sub-paragraphs); 1.2. suspend in accordance with point 1.1. the use of such cameras until the lawfulness of the use of the cameras has been proven to the Inspectorate. If Pallimehed OÜ suspends the use of cameras, but wishes to continue using the cameras at the workplace, the Inspectorate must be proven to comply with the principles of personal data processing (legality and transparency) (see Section 2 of the Recitals of the Data Protection Inspectorate). Further use of the cameras is permitted only if Pallimehed OÜ has certified the lawfulness of the use of the cameras to the Inspectorate and the Inspectorate has sent a confirmation to Pallimehed OÜ regarding the permissibility of the use of the cameras (see item 1 and item 2 2. Send a confirmation to the Inspectorate whether: 2.1. the cameras have been removed and further data processing has been completed or; 2.2. the use of the cameras has been temporarily suspended (pending verification of the lawfulness of the use of the cameras). Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 3. To inform the employees: 3.1. infringement related to the use of cameras (see Section 3 of the Inspectorate's explanatory memorandum for more details); 3.2. the decision to suspend or terminate the use of the cameras (see Section 3 of the Inspectorate's explanatory memorandum for details). 4. Send a confirmation to the Inspectorate that the employees have been notified of the violation and the decision to suspend or terminate the use of the cameras. We set the deadline for compliance with the precept as 17.09.2021. Notify the Data Protection Inspectorate to the e-mail address info@aki.ee of the fulfillment of the precept by the deadline. CONTEST REFERENCE: This precept can be challenged within 30 days by submitting either: - a challenge under the Administrative Procedure Act to the Data Protection Inspectorate, or - an appeal to the Tallinn Administrative Court under the Code of Administrative Court Procedure (in which case the challenge can no longer be heard). Contestation of a precept does not suspend the obligation to comply with the precept or the application of the measures necessary for compliance. PENALTY

WARNING: If a precept is not complied with by the specified term, the Data Protection Inspectorate shall impose a penalty payment on the addressee of the precept on the basis of § 60 of the Personal Data Protection Act for each item of the precept not complied with. The penalty payment may be imposed repeatedly - until the precept is complied with. If the addressee does not pay the penalty payment, it is forwarded to the bailiff to start enforcement proceedings. In this case, the bailiff's fee and other enforcement costs are added to the penalty payment. WARRANTY PENALTY WARRANTY: Misdemeanor proceedings may be instituted for failure to comply with a precept pursuant to Article 58 (1) of the General Data Protection Regulation on the grounds of § 70 of the Personal Data Protection Act. A natural person may be fined up to EUR 20 000 000 for this act and a legal person may be fined up to EUR 20 000 000 or up to 4% of its total annual worldwide turnover, whichever is greater. The Data Protection Inspectorate conducts extra-judicial proceedings against misdemeanors. FACTUAL CIRCUMSTANCES: The Data Protection Inspectorate (Inspectorate) received an application stating that Pallimehed OÜ has installed the cameras, but has not explained to the employees why they are needed. At the same time, the address indicates that the cameras are being used to count the operating hours. Based on the above, we initiated supervision proceedings on the basis of clause 56 (3) 8) of the Personal Data Protection Act. In order to find out whether the use of the cameras complies with the requirements of the General Regulation on the Protection of Personal Data, the Inspectorate sent an inquiry to Pallimehed OÜ in case number 2.1.-1/21/1116 in the course of the supervision procedure In the inquiry, we wanted to: 1. State all the purposes of using the cameras. Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 2. On what legal bases do the cameras are used pursuant to Article 6 (1) of the CISA? 3. If the cameras are used on the basis of, inter alia, Article 6 (1) (f) (legitimate interest) of the CISA, submit to the Inspectorate a thorough analysis of the legitimate interest on the basis of which the lawfulness of the use of the cameras can be assessed. 4. Provide all documents governing the use of the cameras that have been made available to employees. If the document is not limited to the use of cameras, please refer to the specific points in the document that specifically govern the use of cameras. 5. Whether and how employees have access to the analysis of legitimate interests referred to in point 3. In the inquiry, the Inspectorate also drew attention to the imposition of a precept and a penalty payment if the Inspectorate's inquiry is not answered in time. As Pallimehed OÜ did not respond to the inquiry of the Inspectorate, on 15.07.2021 the Inspectorate issued a precept-warning to Pallimehed OÜ in case no. 2.1.-6/21/19, in which we undertook to respond to the inquiry. 15.07.2021 Pallimehed OÜ sent the following reply to the Inspectorate: We received your letter on 15.07. We apologize for not responding to the first precept. Namely, the first letter was

sent to pallimehed@hot.ee by e-mail. This email is being managed by employees, not board members. We had not received the first letter. Pallimehed OÜ has really installed cameras in February 2021 xxx. Employees and the company manager xxx were informed about this activity. A general meeting was also held in February to explain the installation of the cameras. Cameras are needed to check the goods on / off. In addition for security purposes. Cameras are not used to record employee hours. As the goods move through the corridor and one office (xxx) on a daily basis, disputes have arisen with customers over the delivery note and the quantities of the goods. With the help of these cameras it is possible to identify the quantities of goods. In addition, xxx is also in one workspace for security purposes. On 15.07.2021, a member of the company's management board informed all other employees by e-mail about the existence and necessity of the cameras. Although Pallimehed OÜ sent an answer to the Inspectorate on 15.07.2021, only one question submitted in the inquiry sent on 19.05.2021 was answered. Therefore, on 02.08.2021, the Inspectorate sent a notice regarding the fulfillment of the precept, in which we stated the following: on what legal bases are cameras used? s 2. If the cameras are used on the basis of, inter alia, Article 6 (1) (f) of the CCIP (legitimate interest), submit to the Inspectorate a thorough analysis of the legitimate interest on the basis of which the legality of the use of the cameras could be assessed. 3. Submit all documents governing the use of the cameras. 4. Whether and how employees have access to the analysis of legitimate interests referred to in point 2. If Pallimehed OÜ does not provide specific answers to all the questions in the inquiry by the specified deadline (25.08.2021) and the requested documents are not forwarded or the cameras are not removed, the Supervision Authority has the right to impose a penalty payment of up to 5,000 euros. Also in a situation where Pallimehed OÜ is unable to prove to the Inspectorate the compliance with the requirements of IKÜM, incl. The existence of a legal basis Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 make an additional order to remove the cameras. In addition, we explained in a document sent on 02.08.2021 which requirements and how to meet the camera when using it. EXPLANATION OF THE PERSONAL DATA PROCESSOR On 09.08.2021, Pallimehed OÜ sent the following answer to the Inspectorate: 2. Article 6 (1) (F) shall not apply. 3. The use of cameras has been introduced orally to employees as well as in writing by e-mail. This material is attached. Employees have been informed that this recording is only available to board members and will expire 48 hours after recording. 4. Employees can contact the members of the board if they are interested, and we can present the camera image, program and recording from a computer. In addition, a copy of the notification was sent to the Inspectorate, which was forwarded to the employees: Cameras installed in February xxx. At the general meeting in February, you were

informed about this topic. We confirm that these cameras will not be used to monitor you. The camera is needed to check the goods on / off and for security purposes. GROUNDS FOR THE DATA PROTECTION INSPECTORATE: 1. Processing of personal data Personal data is any information about an identified or identifiable natural person. An identifiable natural person is a person who can be identified, directly or indirectly. With the help of cameras, a person (especially an employee) can be identified in any case. Thus, the use of cameras is a processing of personal data, which must comply with the requirements set out in the General Regulation on the Protection of Personal Data (EDPS). The controller (employer) must follow the principles set out in Article 5 (1) of the CISA when processing personal data (including the use of cameras). Compliance with these principles is and must be the responsibility of the controller himself (see Article 5 (2) of the CCIP). To the extent that the processing does not fully comply with the principles set out in Article 5 (1) of the CISA or the controller is unable to demonstrate compliance with those principles, the processing shall also be prohibited. 2. Principles of personal data processing As mentioned above, the controller must comply with the principles set out in Article 5 (1) of the CISA when processing personal data (including the use of cameras) and the controller must comply with these principles (see Article 5 (2) CISA). In the following, we present the principle of processing personal data, the question raised in the inquiry of the Inspectorate, the answer of Pallimehed OÜ and the assessment of compliance with the requirements of IKÜM. 2.1. Processing is lawful (Article 5 (1) (a) CISA) The processing of personal data is lawful only if at least one of the conditions set out in Article 6 (1) CISA is met, and only to the extent that this condition is met (see Article 6 (1) CISA). ). Only the employer can and must justify whether and on what legal basis the cameras are used. Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 2.1.1. In the framework of the supervision procedure, the Inspectorate wanted to know the following: 1. On what legal bases do the cameras are used pursuant to Article 6 (1) of the CCIP? 2. If the cameras are used, inter alia, on the basis of Article 6 (1) (f) (legitimate interest) of the CISA, submit to the Inspectorate a thorough analysis of the legitimate interest on the basis of which the lawfulness of the use of the cameras can be assessed. 2.1.2. Pallimehed OÜ answered the questions of the Inspectorate as follows: 1. Pursuant to Article 6 (1), it has been complied with on the basis of point (b). 2. Article 6 (1) (F) shall not apply. 2.1.3. Pursuant to Article 6 (1) (b) of the CISA, personal data may be processed only if the processing of personal data is necessary for the performance of a contract concluded with the participation of the data subject. Using a camera to perform a contract is necessary, for example, on a television where the work involves being in the camera's field of view. However, Article 6 (1) (b) CISA does not cover situations where the processing is not actually necessary for the

performance of the contract but has been undertaken unilaterally by the controller with regard to the data subject. In other words, based on the performance of the contract, it is not possible to install cameras to check in / out the goods and for security purposes. Processing of such data is permitted only under Article 6 (1) (f) (legitimate interest) of the CISA, provided that the conditions of that provision are fully met. We also repeat the following in the document sent on 02.08.2021: If Pallimehed OÜ uses a legitimate interest as a legal basis for cameras, we emphasize that in order to be able to rely on a legitimate interest, all three conditions must be met at the same time: 1) The controller or third party interest; 2) the processing of personal data is necessary for the exercise of a legitimate interest; (3) The legitimate interests of the controller and / or of a third party outweigh the interests or fundamental rights and freedoms of the data subject protected. The possibility of using this legal basis and its assessment can be divided into three stages, ie firstly the legitimate interests and weight of the data controller, secondly the rights and interests of the data subject (employees, partners, customers) and thirdly the consideration of conflicting interests, including preliminary assessment + additional safeguards and a final assessment. In the light of the above, the controller has an obligation to weigh the legitimate interests of himself and / or the third party against the interests and fundamental rights of the data subject, as a result of which Article 6 (1) (f) CISA can be invoked as a legal basis for processing. The fact that the processor has a legitimate interest in the processing of personal data does not automatically mean that the processor can rely on Article 6 (1) (f) of the CCIP. The legitimacy of the controller's interest is only a starting point, ie one of the elements to be analyzed, and whether the basis of a legitimate interest can be relied on depends on the outcome of the balancing act. It is for the controller to ascertain whether the legitimate interest provision can be relied on, who must carry out the weighing in a transparent manner and be able to justify it. Thus, in order to understand whether personal data can be processed on the basis of Article 6 (1) (f) of the CISA, Pallimehed OÜ must prove whether and what is the legitimate interest of the company. Legitimate interests must be sufficiently clear. This requires a real and present interest - something related to an ongoing activity or a benefit that is expected to accrue in the near future. Perhaps it is necessary to explain, among other things, what is meant by security and how cameras ensure the purpose of security. In other words, interests that are too vague or speculative are not enough. If legitimate interests are not sufficiently clear, these interests cannot be balanced against the interests and fundamental rights of the data subject. Therefore, it is important that the legitimate interest is sufficiently worded in accordance with the applicable legislation, Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 and real and current not speculative). Secondly, it is necessary to analyze

the possible interests or fundamental rights of the data subject - and the freedoms that may be affected by the processing of personal data. Third, the legitimate interests of Pallimehed OÜ must be balanced with the interests and fundamental rights of the data subject. The impact of the processing (collection, use, storage) of personal data on the data subject is compared with the legitimate interests of the controller and it is assessed whether and to what extent the legitimate interests of the controller outweigh the interests of the data subject. It must also be borne in mind that employees should not normally be in sight of the camera throughout their working hours and that the employer should make every effort to achieve his or her legitimate interests and objectives with the least possible measures. In addition, it must be considered whether the cameras can only be switched on during non-working hours for safety reasons and the inspection of the consignment note / goods must be carried out in a place where workers are not normally present during normal working hours. If the data controller fails to carry out one of the previous steps correctly, the processing of the data is not permitted under Article 6 (1) (f) of the CISA and the further processing of personal data is unlawful. However, the assessment and documentation of a legitimate interest is the responsibility of the camera user (controller). We have also explained the assessment of a legitimate interest in a separate guide. The analysis of legitimate interests must also be included in the data protection conditions introduced to employees or be otherwise available to employees (see Article 13 (d) of the IIA). As Pallimehed OÜ has not proved the legality of the use of the cameras to the Inspectorate (it has not provided a legal basis, the conditions of which have been met when using the cameras), further use of the cameras is prohibited. If the use of the cameras is stopped (the cameras are removed), a confirmation must be sent to the Inspectorate. However, if the use of cameras is suspended pending verification and verification of their legality, the Inspectorate must be provided with an analysis of the legitimate interest in accordance with the above conditions, on the basis of which the Inspectorate will assess whether or not the use of cameras is permitted. 2.2. Processing is transparent to the data subject (Article 5 (1) (a) CISA) The principle of transparency presupposes that all information and messages relating to the processing of personal data are easily accessible, comprehensible and clearly worded. In other words, data protection conditions must be in place. The content of the data protection conditions is governed by Articles 12 to 14 of the CISA. 2.2.1. As part of the supervision procedure, the Inspectorate wanted to know the following: 3. To forward all documents regulating the use of cameras and which have been introduced to employees. If the document is not limited to the use of cameras, please refer to the specific points in the document that specifically govern the use of cameras. 4. Whether and how employees have access to the analysis of legitimate interests referred to in point 3. 2.2.2. Pallimehed OÜ

answered the questions of the Inspectorate as follows: 3. The use of cameras has been introduced orally to employees, as well as in writing by e-mail. This material is attached. Employees have been informed that this recording is only available to board members and will expire 48 hours after recording. 4. Employees can contact the members of the board if they are interested, and we can present the camera image, program and recording from a computer. In addition, a copy of the notification was sent to the Inspectorate, which was forwarded to the employees: Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 Cameras installed in February xxx. At the general meeting in February, you were informed about this topic. We confirm that these cameras will not be used to monitor you. The camera is needed to check the goods on / off and for security purposes. 2.2.3. We explain that informing employees about the use of cameras does not meet the requirements set out in the IKÜM. We repeat here 02.08.2021: Here we also point out that according to Article 5 (1) (a) of the CISA, the processing of personal data must be transparent. The principle of transparency presupposes that all information and messages related to the processing of personal data are easily accessible, comprehensible and clearly worded. In other words, data protection conditions must be in place. The content of the data protection conditions is governed by Articles 12 to 14 of the CISA. b) The purposes and legal basis for the processing of personal data; (c) Where the processing of personal data is based on a legitimate interest, an analysis of the legitimate interest or information on how the analysis of the legitimate interest can be consulted; d) Term of storage of camera recordings; (e) Information about the right to request access to and request the deletion of the recordings concerning him or her or to restrict the processing of personal data or to object to the use of the camera; f) Information on the right to lodge a complaint with the supervisory authority (Data Protection Inspectorate). The Inspectorate outlined the main requirements for using the camera to compile data protection conditions, but Pallimehed OÜ must still review the requirements set out in Article 13 (1) and (2) of the IPCM and draw up the correct data protection conditions. Considering that Pallimehed OÜ has not prepared and forwarded the data protection conditions to the Inspectorate and has not informed the employees about the use of the cameras in accordance with the requirements of the IKÜM, Pallimehed OÜ must immediately prepare data protection conditions that meet the requirements of Article 13 of the IKÜM. The prepared conditions must also be forwarded to the Inspectorate in due time. 3.3. In summary, we note that the responsibility for proving that the notification of the processing of personal data (use of the camera) is transparent and meets the requirements set out in Articles 12-13 of the CCP rests with Pallimehed OÜ (see Article 5 (2) of the CCIP). In a situation where Pallimehed OÜ does not submit the correct data protection conditions to the Inspectorate and they are not introduced to

the employees, the cameras must be removed until the processing of personal data (use of the cameras) is transparent to the employees. Considering that the data protection conditions have not been forwarded to the Inspectorate and, according to the materials of the case, the employees have not been informed about the use of the cameras in accordance with the requirements of the IKÜM, the use of the cameras is illegal. Therefore, further use of the cameras is prohibited. If the use of the cameras is stopped (the cameras are removed), a confirmation must be sent to the Inspectorate. If the use of the cameras is suspended, the data protection conditions in accordance with Articles 12 to 13 of the CISA must be communicated to the Inspectorate, on the basis of which the Inspectorate will assess whether the use of the cameras is transparent to employees. 3. Informing employees The use of cameras constitutes a very serious invasion of privacy, so it is particularly important that in cases where the cameras have been installed illegally, ie did not comply with the principles of personal data processing (including legality and transparency), the cameras are removed immediately and also notified (see Article 34 (1) of the CCIP). Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 The breach notification shall describe the nature of the personal data breach in clear and simple language and provide at least the following information (see Articles 34 (2) and 33 (3) of the CISA) ): 1. Name and contact details of the contact person from whom further information regarding the infringement can be obtained; 2. Describe the possible consequences of the personal data breach; 3. Describe the measures taken or planned to address the personal data breach. In order to terminate the further violation immediately, Pallimehed OÜ must either suspend or terminate the use of the cameras. If the use of the cameras is suspended, the continued use of the cameras is permitted only if the Inspectorate has checked the legality of the use of the cameras and confirmed to Pallimehed OÜ that the use of the cameras is permissible. The decision to suspend or terminate the use of the cameras must also be set out in a notice to employees. Otherwise, employees must continue to work in the knowledge that their activities will be recorded illegally. Summary In view of the above, Pallimehed OÜ has not proved that the use of cameras complies with the principles of personal data processing provided for in Article 5 (1) of the CISA, ie the processing of personal data is lawful and transparent. Compliance with these principles is the responsibility of the controller himself (see Article 5 (2) of the CISA). If the processing of personal data does not comply with the principles set out in Article 5 of the CISA or the controller is unable to prove this, the processing of personal data shall be prohibited. Thus, Pallimehed OÜ must either: 1) stop using those cameras in which the employees are also in sight, or; 2) suspend the use of cameras until the lawfulness of the use of cameras has been proved to the Inspectorate and the Inspectorate has confirmed the lawfulness of the use of cameras.

Pursuant to § 58 (1) of the Personal Data Protection Act and Article 58 (2) (e) and (f) of the General Data Protection Regulation, the Supervision Authority has the right to order the controller to notify the data subject of a personal data breach and to impose a temporary or permanent restriction on processing. Thus, the Inspectorate also has the right to impose a temporary or permanent restriction on the use of cameras, including a ban on processing. Taking into account the factual circumstances, including the fact that Pallimehed OÜ has installed the cameras, but Pallimehed OÜ has not proved that the requirements of IKÜM (Articles 5, 6, 12 and 13) have been met, the Inspectorate finds that issuing a mandatory precept to terminate or suspend the use of cameras is In this case, it is necessary to put an end to the infringement as soon as possible. / digitally signed / Raiko Kaur, lawyer, authorized by the Director General