PRIVACY PROTECTION AND STATE TRANSPARENCY Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 PRESCRIPTION-WARNING in personal data protection case No. 2.1.-5/23/120-4 Prescription issued by the Data Protection Inspectorate jurist Jekaterina Aader Time and place of issuing the injunction 27.03.2023 in Tallinn Recipient of the injunction - personal data processor XXXX personal code: XXXXX address: XXXXX RESOLUTION: § 56 (1), (2) point 8, § 58 (1) of the Personal Data Protection Act and § 58 (1) of the Personal Data Protection Act (IKÜM) on the basis of Article 58 paragraph 2 points a and f, Article 5 paragraph 1 point a, Article 6 paragraph 1 point f, I issue a mandatory order for compliance: 1. stop processing personal data using cameras, including by changing the field of view of already installed cameras so that the field of view is not remain in any public or common area, and send confirmation of this (e.g. screenshots of the cameras) to the e-mail address info@aki.ee or stop processing personal data with the help of cameras outside the real part of the apartment property, including removing already installed cameras and sending pictures of the locations where the cameras were removed to the inspection, at the e-mail address info@aki.ee. 2. delete the existing recordings and send confirmation of this to the inspection at info@aki.ee. I set the deadline for the execution of the order to be 12.04.2023. Report compliance with the order to the Data Protection Inspectorate by this deadline at the latest. REFERENCE FOR DISPUTES: This order can be challenged within 30 days by submitting either: - an appeal under the Administrative Procedure Act to the Data Protection Inspectorate or - an appeal under the Code of Administrative Procedure to the Administrative Court (in this case, the appeal in the same matter cannot be reviewed). Challenging a precept does not stop the obligation to fulfill it or the implementation of measures necessary for fulfillment. EXERCISE MONEY WARNING: If the injunction has not been complied with by the specified deadline, the Data Protection Inspectorate will impose an extortion fee of 1,000 euros for each point of the unfulfilled injunction to the addressee of the injunction based on § 60 of the Personal Data Protection Act. A fine may be imposed repeatedly - until the injunction is fulfilled. If the recipient does not pay the penalty, it will be forwarded to the bailiff to start enforcement proceedings. In this case, the bailiff's fee and other enforcement costs are added to the enforcement money. MISCONDUCT PUNISHMENT WARNING: Failure to comply with the prescription under Article 58(2) of the Personal Data Protection General Regulation may result in a misdemeanor proceeding based on § 69 of the Personal Data Protection Act. For this act, a natural person may be fined up to EUR 20,000,000, and a legal person may be fined up to EUR 20,000,000 or up to 4 percent of its global annual turnover of the previous financial year, whichever is greater. The out-of-court procedure for a misdemeanor is the Data Protection Inspectorate. FACTUAL CIRCUMSTANCES: On

16.01.2023, the Data Protection Inspectorate received a complaint regarding surveillance cameras installed on both sides of the window opening on the exterior facade of apartment XX of Rae tn. According to the applicant, the owner of the apartment has also installed cameras in the past, but removed them after a conversation with the regional police officer. By the time the complaint is filed, video surveillance has been reinstated. According to the complaint, the residents of the building feel that their privacy is being violated and want the cameras to be dismantled. On 13.02.2023, the inspection sent an inquiry to the camera owner (data processor) and a proposal to remove the cameras installed on both sides of the window opening of apartment XX on the exterior facade of the apartment building at Rae tn 31, to delete the existing recordings and to submit a confirmation of the completion. As an alternative demand, the inspectorate proposed to stop the filming of public areas until a legitimate interest analysis and data protection conditions have been drawn up regarding the use of the camera, they have been forwarded to the Data Protection Inspectorate together with screenshots of the camera image, and the inspectorate has confirmed their legality. In the event that the camera owner finds that he has met all the conditions for using the camera, the inspectorate asked to submit a confirmation from the apartment association that allows the installation of cameras on the exterior facade, photos of the camera image (screenshots) and an analysis of the legitimate interest in filming the public area together with the conditions for using the cameras. The inspection set 27.02.2023 as the deadline for completing the proposal. However, the data processor has not responded to the inspection's proposal, which is why issuing an injunction is inevitable. On 01.03.2023, the inspection determined that the owner of apartment XX in the Rae tn 31 apartment building, in addition to the previous cameras, installed another stationary camera under the ceiling above his apartment door, facing the common area of the staircase on his floor. PERSONAL DATA PROCESSOR'S EXPLANATION: The data processor failed to respond to the inspection's proposal and did not explain the legal basis for the use of stationary cameras, the purpose of filming, necessity, scope, data processing conditions and other circumstances. In addition, the data processor installed a third stationary camera under the ceiling above his apartment door, pointing to the territory of the stairwell on his floor. GROUNDS OF THE DATA PROTECTION INSPECTION: Basics of personal data processing 1. According to article 4 point 1 of the GDPR, personal data is any information about an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be directly or indirectly identified, in particular on the basis of an identification feature such as name, social security code, location information, network identifier or on the basis of one or more physical, physiological, genetic, mental, economic, cultural or social characteristics of that natural person. Therefore, personal data is, among other

things, an image of a person transmitted by a camera, if the person can be identified. A person is identifiable even if his face is not visible on the camera image; it is possible to recognize the person through his other characteristics (e.g. body shape, clothing, belongings, special signs of feeling, etc.). According to Article 4, point 2 of the IKÜM, the processing of personal data is an automated or non-automated operation or a set of operations performed with personal data or their collections, including their distribution or disclosure by making them available in another way. Therefore, monitoring and recording with a camera is also processing of personal data. Thus, the data processor processes personal data when monitoring and recording with the camera. The processing of personal data takes place regardless of whether the recordings are reviewed or not. 2. According to article 5 paragraph 1 point a of IKYM, when processing personal data, it is ensured that the processing is legal, fair and transparent to the data subject. Pursuant to Article 6(1) of IKÜM, the processing of personal data is legal if it meets one of the conditions listed in Paragraph 1(a) to (f). In the case of the bases provided in points a-e of Article 6, paragraph 1 of the GDPR, the legality of data processing is based on the data subject's consent, contractual orders, statutory obligation or other specific reason defined in the legislation. In this case, the aforementioned grounds for personal data processing do not exist. Thus, data can be processed with tracking devices (including stationary cameras) only on the basis of the legitimate interest provided for in Article 6(1)(f) of the IKÜM. Legitimate interest does not need to be assessed by an individual data processor if he uses a stationary security camera and only the area in his own exclusive use, not a public or shared space (e.g. street, stairwell of an apartment building, next door) remains in its field of view. Exception for personal purposes 3. Point 18 of the IKÜM preamble explains that the general regulation should not be applied to the processing of personal data carried out by a natural person exclusively for personal or domestic purposes and therefore outside of professional or business activities. The exception for personal use only applies when filming an area you own (e.g. your own apartment, apartment door, etc.). In the 2014 decision C-212/13 of the European Court of Justice, it was found that the use of a camera system installed by a natural person on a private house for the protection of property and persons does not take place only for personal purposes, if such a system also monitors a public space (e.g. a public street) or someone else's property, then, according to the court's decision, it is no longer treated as filming for personal purposes, and there is no basis for filming outside the property area. For example, if a person films his private road, but it has been given to public use or an easement has been set up for the benefit of someone else, then the exception for personal use can no longer be relied upon. According to the judgment of the European Court, a stationary camera contains the risk of profiling people (the camera may repeatedly monitor the activities of a specific person in the field of

view of the camera)1. Therefore, there is no legal basis for filming public or public spaces and properties belonging to other persons, which would allow them to infringe on their right to privacy. The apartment owner of Rae tn 31-XX installed two stationary cameras facing outside the apartment on the exterior facade of the apartment building on both sides of his window opening, the field of view of which includes the public space (including the front of the house, green area, stairwell, street), and one stationary camera under the ceiling above the door of his apartment facing the common area of the stairwell, which means that people passing by the camera, including residents and guests of the apartment building, will inevitably be in the field of view of the cameras. In such a case, it cannot be a matter of data processing only for personal purposes, and the camera owner must consider whether he has fulfilled the conditions of a legitimate interest arising from Article 6, paragraph 1, point f of IKÜM, to film it, and to use signs informing about the camera (IKÜM art. 13). Legitimate interest analysis 4. Pursuant to IKÜM Article 6(1)(f), the processing of personal data is legal if it is necessary for the legitimate interest of the data controller or a third party, unless such interest is outweighed by the interests of the data subject or the fundamental rights and freedoms of personal data must be protected. In order for a legitimate interest to be relied upon, all three conditions must be met at the same time: 1) the controller or a third party has a legitimate interest in data processing; 2) the processing of personal data is necessary for the exercise of a legitimate interest, i.e. there is no other effective but less privacy-intrusive measure to achieve the same goal; 3) the legitimate interests of the controller and/or a third party outweigh the interests or fundamental rights and freedoms of the protected data subject. Based on the aforementioned, in order to determine the possibility of processing personal data on the basis of Article 6(1)(f) of the IKÜM, the camera owner must prove whether and what his legitimate interest is in filming a public area, then whether filming is necessary for the exercise of his legitimate interest and, finally, whether filming outweighs the rights of individuals. 5. Legitimate interests must be formulated clearly enough so that it can be balanced with the interests and fundamental rights of the data subject. In addition, the interest at stake must be that of the controller. This requires a real and present interest – something related to an activity currently taking place or a benefit expected to be received in the near future. In addition, the interest can be considered legitimate as long as the controller can implement the interest in a manner that is consistent with data protection and other legislation. In other words, the legitimate interest must be permissible by law.2 Also in the case of video surveillance, the legitimate interest must actually exist and it must be an actual issue (ie it must not be fictitious or speculative). Before starting surveillance activities, the real situation must be present, for example previous damage or previous serious incidents.3 1 of the European Court of Justice of December 11, 2014. reference

for a preliminary ruling in the case of František Ryneš v Úřad pro ochranu środnyk dátní, application no C-212/13. 2 Opinion 06/2014 on the concept of legitimate interests of the data controller in the sense of Article 7 of Directive 95/46/EC. 3 Guidelines of the European Data Protection Board 3/2019 on the processing of personal data in video devices (Guidelines for Video Surveillance), p. 10, p. 20. Therefore, it is important that the legitimate interest is: - in accordance with current legislation - formulated clearly enough (i.e. sufficiently specific) - and real and currently occurring (ie not speculative). Secondly, before using the camera system, the controller is obliged to assess where and when video surveillance measures are absolutely necessary. Namely, before installing a video surveillance system, the data controller should always critically examine whether this measure is firstly suitable (it is possible to achieve the set goal with the measure) to achieve the desired result and secondly sufficient and necessary to achieve these goals. Video surveillance measures should be chosen only if the purpose of the processing cannot reasonably be achieved by other means that are less intrusive to the fundamental rights and freedoms of the data subject. Generally, the need to use video surveillance to protect the property of the data controller ends at the borders of the property. 4 Thirdly, the data processor must analyze the possible interests or fundamental rights and freedoms of the data subject that may be harmed by the processing of personal data, and balance the legitimate interests of the data processor with the interests and fundamental rights of the data subjects. The controller must consider 1) the extent to which the monitoring affects the interests, fundamental rights and freedoms of individuals and 2) whether it causes a violation of the data subject's rights or negative consequences for his rights. Balancing interests is actually a must. It is necessary to carefully assess and balance the fundamental rights and freedoms on the one hand and the legitimate interests of the controller on the other.5 It is important to keep in mind that the legitimate interests of the controller or a third party do not automatically outweigh the interests related to the fundamental rights and freedoms of the protected data subjects. If the data processor considers that his legitimate interest is compelling, but the encroachment on the rights of the data subject is also compelling, the implementation of various protective measures must be considered, such as a shorter retention period, recording only at night, etc. If the data processor fails to perform one of the previous steps correctly, data processing is not permitted on the basis of Article 6(1)(f) of the IKÜM, and the inspectorate has the right to prohibit further processing of personal data. Assessment of legitimate interest is the responsibility of the camera owner (data processor)6. It must also be taken into account that the analysis of the legitimate interest must be documented and it must be possible for any person to get acquainted with it (Article 13, paragraph 1, point d of the ACT). 6. The data processor failed to analyze the legitimate interest in

filming the public area with the cameras installed in the apartment building on Rae Street 31, as a result of which the use of cameras filming the public area is not permitted based on Article 6(1)(f) of the IKÜM. The use of cameras must be stopped until a correct legitimate interest analysis has been prepared regarding the filming of public spaces, which will reveal whether and to what extent (e.g. in which places more precisely) video surveillance can be used. Notification and data protection conditions 7. Pursuant to Article 13 of IKÜM, the responsible data processor informs the person of all the information prescribed in Article 13 at the time of receiving personal data. In the case of video surveillance, the most important information should be provided on the notification label: the purpose of the processing, the legal basis, the name of the controller and contact details. In addition to the correctly installed label, it is also necessary to prepare data protection conditions. The camera notification label should be placed so that a person can easily reach the monitored area 4 Video surveillance guidelines, p. 10-11, p 24-27. 5 Video surveillance guidelines, p. 11, p. 30. 6 IKÜM art. 5 par. 2 and art. 12-14, see also justification point 76. to become aware of camera surveillance when entering. There is no need to indicate the location of the camera unless there is any doubt as to which areas are being monitored. A person must be able to estimate which area is in the camera's field of view, so that he can avoid surveillance or adjust his behavior if necessary.7 8. One of the criteria for the legality of personal data processing in Article 5 paragraph 1 point a of the IKÜM is to ensure the transparency of data processing, namely that all information and messages related to personal data processing must be easily accessible, understandable and clearly worded. This means that the camera owner must also prepare data protection conditions when processing other people's personal data. The content of the data protection conditions is regulated by articles 12 - 14 of the IKÜM. The data processor must provide all the information stipulated in articles 13 -14 of the IKÜM in the data protection conditions8. In a situation where video surveillance is used, the data protection conditions or the video surveillance procedure must be based on Article 13 of the IKÜM, i.e. the conditions must reflect, among other things, the following: - the purposes and legal basis of personal data processing; - legitimate interest analysis or information on how it is possible to consult the legitimate interest analysis; - recipients of personal data (e.g. name of authorized processor); - period of storage of personal data (term of storage of camera recordings); - information on the right to request access to personal data and their correction or deletion or restriction of processing of personal data and to object to the processing of such personal data, as well as information on the rights to transfer personal data; - information on the right to file a complaint with the supervisory authority. It can be seen from the image material that there are no signs informing about video surveillance above the cameras on the

exterior facade of the apartment building on Rae tn 31 in Paldiski and the camera under the ceiling above the door of apartment XX. Thus, the camera owner failed to fulfill the notification obligation of the data processor. Retention of camera recording 9. According to Article 5(1)(c) and (e) of the IKÜM, personal data may not be stored longer than is necessary for the purposes for which they are processed. In its guidelines 3/2019 on the processing of personal data in video devices, the European Data Protection Board has stated the following:9 "Taking into account the principles set out in Article 5(1)(c) and (e) of the General Regulation on Personal Data Protection, namely the collection of as little data as possible and the limitation of storage, personal data should in most cases (e.g. vandalism for discovery) to be deleted - ideally automatically - after a few days. The longer the prescribed retention period (especially if it is longer than 72 hours), the more the legitimacy of the purpose and the necessity of retention must be justified. If the controller uses video surveillance not only to monitor its premises, but also intends to store the data, the controller must ensure that the storage is actually necessary to achieve the purpose. If storage is necessary, the storage period must be clearly defined and established separately for each specific purpose. The controller is responsible for determining the retention period in accordance with the principle of necessity and proportionality and for proving compliance with the provisions of the General Regulation on the Protection of Personal Data. Therefore, in a situation where a longer retention period does not arise from the special law, the retention period of 72 hours should generally be used. It is important to note that the longer the recordings are kept, the greater the impact on the individuals caught in the recordings. 7 Video surveillance guidelines, p. 26, p 113. 8 See also Article 29 working group guidelines on transparency under Regulation 2016/679, p. 35-40. 9 Video surveillance guidelines, p. 28, p. 121. 10. IKÜM Article 32 paragraph 1 obliges the authorized processor to ensure the security of data processing. The organizational and technical measures taken must be proportionate to the threats to the rights and freedoms of natural persons resulting from the accidental or illegal destruction, loss, alteration and unauthorized disclosure or access to video surveillance data.10 It is especially important to ensure that outsiders do not gain access to video recordings, and there would be no unauthorized disclosure of personal data. Access to the camera image must be justified and the purpose of using the recording must be clear (IKYM art. 5 paragraph 1 points a-b). In order to be able to check afterwards who, when and which video recording has been viewed, a logging system must be created. According to the inspection, logging is the only possible way to check that the camera's live image or recordings have not been viewed illegally, including without reason. 11. When using cameras, the data processor must also take into account the person's right to receive data collected about him or her, i.e. extracts from video

recordings. The data processor has the obligation to respond to the requirements for viewing the video recordings within 30 days.11 In addition, on the basis of Art. 17 of the General Regulation on the Protection of Personal Data (IKÜM), the person has the right to demand from the data processor, i.e. the cooperative, the deletion of his data (in this case, the video recordings). Use of cameras in an apartment building 12. Pursuant to subsections 3 and 4 of § 4 of the Apartment Ownership and Apartment Association Act (KrtS), all parts of the building that are not part of an item of special property, i.e. an apartment (including equipment necessary for the building's maintenance or safety within the apartment or for the common use of apartment owners) are jointly owned by apartment owners. The exterior facade of the apartment building, the staircase, the common corridor, the elevator, etc. are also the joint property of the apartment owners. The rules for the use of co-ownership parts are established by the apartment association (KrtS § 12 subsection 1). Therefore, the apartment owners can also decide on the use of the video surveillance system jointly, and the corresponding decision can be adopted at the general meeting with a majority vote (KrtS § 20). The apartment association has the option to decide that it is not allowed to install cameras in the house arbitrarily. It can also be agreed that the board of the cooperative will dismantle the arbitrarily installed cameras and return them to the owner, if the person has not done so himself after the warning, etc. granted permission for the use of a video surveillance system in the co-owned parts of the apartment building, including the installation of cameras in the building, and the data processor has not forwarded the corresponding permission to the inspection. Without the decision of the general meeting of the apartment association, installing cameras on the common property parts and filming with them is against the law and does not comply with the principle of legality of data processing (IKÜM art. 1 paragraph 1 point a). Summary 13. Based on the above, in order for the apartment building to be able to use video surveillance and monitor the public space or the common area of the apartment building with cameras, the data processor must meet the following requirements: 1) obtain permission from the apartment association (decision of the general meeting) to install cameras and video surveillance in the co-owned parts of the apartment building (see point 12 of the reasons for the inspection); 10 Video surveillance guidelines, p. 28, p. 123. 11 IKÜM article 15. 12 Tallinn District Court's decision of 15.11.2018 in civil case no. 2-16-12460 found that such a rule does not harm the rights of any person, because the rule applies equally to all apartment owners. 2) prepare a correct legitimate interest analysis that meets the conditions set forth in point f of article 6, paragraph 1 of the IKÜM (see points 4-5 of the inspection's reasons); 3) create and install appropriate information signs13 about the use of video surveillance (see point 7 of the inspection's reasons); 4) prepare data protection conditions that fully comply with the requirements stipulated in Articles

12 and 13 of the IKÜM (see points 3 of the inspection's reasons) 5) ensure that the video recordings are deleted immediately, but no later than after 72 hours (see point 9 of the inspection's reasons). A longer retention period must be justified. 14. In conclusion, there is currently no legal basis that would allow the data processor to film the public area and the common area of the apartment building on Rae tn 31 in Paldiski. In addition, there is no decision of the general meeting of the apartment association of Lääne-Harju municipality, Paldiski city, Rae tn 31, which would give permission to the owner of apartment no. XX to use cameras in the shared ownership parts of the apartment building. According to the inspection, the data processor must stop any legal basis of filming public and common areas with cameras, including already installed cameras, and delete all existing recordings. (digitally signed) Jekaterina Aader lawyer under the authority of the general director 13 The notification label can be created using the AKI label generator at the web address videovalvesilt.aki.ee.