PRIVACY PROTECTION AND STATE TRANSPARENCY Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 FOR USE WITHIN THE INSTITUTION Information holder: Data Protection Inspectorate Note made: 12.10.2022 Access restriction valid until: 12.10.2 097; in terms of paragraph 2 until the decision enters into force Basis: AvTS § 35 paragraph 1 paragraph 2, AvTS § 35 paragraph 1 paragraph 12 PRESCRIPTION WARNING in personal data protection case no. 2.1.-5/22/14462 Issuer of the injunction Data Protection Inspectorate lawyer Alissa Hmelnitskaja Time and place of the injunction 12.10.2022 in Tallinn Recipient of the injunction - personal data processor XXX address: XXX e-mail address: XXX RESOLUTION: Paragraph 56 of the Personal Data Protection Act (IKS) 1 and paragraph 2 point 8, § 58 paragraph 1 and Article 58 paragraph 1 point d and paragraph 2 points d and f of the General Regulation on the Protection of Personal Data (IKÜM), as well as taking into account Articles 5 and 6 of the General Regulation on Protection of Personal Data (IKÜM), as well as Articles 5 and 6, the Data Protection Inspectorate issues a mandatory injunction to comply with XXX: 1. terminate filming outside one's property (either by dismantling the camera(s) or directing it so that only one's own property remains). If the cameras are redirected, send photos of the camera image to the Data Protection Inspectorate by e-mail at info@aki.ee to check its scope; 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 injunction as 26.10.2022. Report compliance with the order to the e-mail address of the Data Protection Inspectorate at info@aki.ee 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 is not complied with by the specified deadline, the Data Protection Inspectorate will impose an extortion fee of 800 euros to the addressee of the injunction on the basis of § 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: The Data Protection Inspectorate (AKI) received a complaint from XXX's neighbor regarding the fact that XXX has installed a surveillance camera on the side of his house, which is aimed at the neighbor's property (YYY) and public space. The applicant is not satisfied that the public road and his property are being filmed. The applicant also attached a picture showing a surveillance camera facing a public road. Therefore, the inspection has started the supervision procedure on the basis of IKS § 56 (3) point 8, within the framework of which the inspection submitted a proposal to the data processor in the matter of personal data protection on 23.09.2022. AKI proposed to stop filming the neighboring properties by 30.09.2022 at the latest (either by dismantling the camera(s) or directing them so that only the processor's own property remains) and to delete the existing recordings and to send a confirmation about this to the inspection at info@aki.ee. If the camera(s) are redirected, provide the inspection with photos showing the extent of the camera image. Among other things, the inspection explained to the processor that when filming a public area, in certain cases, the owner can justify the basis of legitimate interest in order to protect his property. On 29/09/2022, XXX responded to the inspection's proposal, sent photos that show the scope of the camera images (4 cameras in total) and confirmed that they have installed cameras on their property that also partially film neighboring properties and the public road. The processor did not provide the inspection with confirmation that it would stop filming neighboring properties and public space or that it would direct the cameras so that only the processor's own property remained. XXX did not convey to the inspectorate a legitimate interest in filming the public area of the analysis, but only pointed out that the cameras were installed in connection with the vandalism that occurred. REASONS FOR THE DATA PROTECTION INSPECTION: 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 directly or indirectly identified (see IKÜM Article 4, point 1). The use of security cameras will inevitably lead to the processing of personal data if people are in the field of view. With the help of cameras, the person can be identified in any case. Therefore, in the case of video surveillance, it is a matter of personal data processing, which must comply with the requirements set forth in the IKÜM. The controller of personal data is obliged to comply with the principles set forth in Article 5, paragraph 1 of the IKÜM. The responsible processor himself is responsible for the fulfillment of these principles and must be able to prove their fulfillment (see IKÜM Article 5 paragraph 2). To the extent that data processing does not fully comply with the principles set forth in Article 5, paragraph 1 of the IKÜM, data processing is prohibited. The use of cameras must be based on, among other

things, the following principles of personal data processing: - Lawfulness, fairness and transparency (Article 5 paragraph 1 point a) of the General Data Protection Regulation. Any processing of personal data must be fair and legal, i.e. fully in accordance with all valid legislation (including IKÜM and IKS). Data processing must also be transparent. The principle of transparency requires that all information related to the processing of personal data is easily accessible, understandable and clearly formulated for the data subject. This primarily concerns the notification of data subjects in order to ensure fair and transparent processing. Informing people is more precisely regulated by articles 12 - 14 of the IKÜM. Articles 13 and 14 of the IKÜM outline what information given to a person must contain as a minimum. The use of cameras must be based on the requirements of Article 13 of IKÜM. - Purpose and retention limitation. Collecting as little data as possible (ICYM article 5 paragraph 1 points b, c and e). In order to assess whether the use of cameras complies with the principle of purpose limitation and the collection of as little data as possible, it is necessary to: 1) state all specific purposes; 2) assess whether the use of cameras is necessary for the fulfillment of the stated goals or whether there are other measures that are less intrusive to the data subject. - Personal data is processed in a way that ensures the appropriate security of personal data, including protection against unauthorized or illegal processing (Article 5(1)(f) of IKÜM) Personal data processing must be stopped and the data deleted or transferred to a non-personalized form if there is no legal basis for personal data processing and/or the objectives have been met , for which they were collected. Based on the principles of purposefulness and collecting as little data as possible, the camera(s) must be directed to specific security risks. 2. Preparing a legitimate interest analysis The processing of personal data is legal only if at least one of the conditions set forth in paragraph 1 of Article 6 of the IKÜM is met. Thus, personal data may be processed if there is a legal basis for this arising from points a - f of Article 6 (1) of the IKÜM. There is a restriction on the use of security cameras for natural persons (or people). The exception for personal purposes only applies when filming an area that belongs to you (e.g. the yard of your own private house). In the 2014 decision C-212/131 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)2. Therefore, there is no legal basis for filming properties belonging to other persons, which would allow them to infringe on their right to privacy. 1 František Ryneš versus Úřad pro ochranu osnych dátní. 2 of the European Court of Justice of December 11, 2014. request for a preliminary ruling in the case of František Ryneš v Úřad pro ochranu osnych dátní, Application No. C-212/13; The data subject, whose personal data is processed, has the right to demand the termination of the processing of personal data, if there is no legal basis for this (IKÜM art. 17 paragraph 1 point d). Therefore, the neighbor of the XXX property, whose rights are infringed by the use of cameras, has the right to demand the termination of the processing of his data. The neighbor has also done this by submitting a complaint to AKI. In such a case, AKI must find out whether the data processing was legal. In the 29.09.2022 response to AKI's proposal, XXX justified that the filming of his property is necessary in connection with the vandalism that took place. According to the inspection, the legal basis for the use of XXX cameras could be derived from IKÜ Article 6(1)(f) only if some part of the public area remains in the camera's field of view, but there is no legal basis for filming the neighbor's property. According to Article 6(1)(f) of IKÜM, the processing of personal data is legal if the processing of personal data 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 for which personal data must be protected . Thus, IKÜM article 6 paragraph 1 point f stipulates three conditions, all of which must be met in order for the processing of personal data to be permitted on the basis of a legitimate interest: - the controller or third parties have a legitimate interest in data processing; - the processing of personal data is necessary for the exercise of a legitimate interest; - the legitimate interests of the data controller and/or third party outweigh the interests, fundamental rights and freedoms of the protected data subject. The possibility of using the said legal basis and its assessment can be graphically divided into three stages, i.e. firstly, the legitimate interests of the personal data processor or third parties and their importance, secondly, the rights and interests of the data subject and their importance, and thirdly, the weighing of conflicting interests, including a preliminary assessment + additional protective measures, if necessary, and a final assessment. Based on the above, the data controller is obliged to compare the legitimate interests of himself and/or a third party with the interests and fundamental rights of the data subject, as a result of which it becomes clear whether it is possible to rely on IKÜ Article 6(1)(f) as the legal basis for processing. If the data processor has a legitimate interest in the processing of personal data, this does not automatically mean that the data processor can rely on Article 6(1)(f) of the IKÜM. The justification of the controller's interest is only a

starting point, i.e. one of the elements that must be analyzed, and whether the legitimate interest can be relied upon depends on the result of the balancing. It is the duty of the controller to make sure whether the provision of legitimate interest can be relied on, who must carry out the consideration in a transparent manner and be able to justify (prove) it. Therefore, in order to understand whether it is possible to process personal data on the basis of Article 6(1)(f) of the IKÜM, XXX must prove whether and what its legitimate interest is and that it outweighs the rights of individuals. Legitimate interests must be formulated clearly enough. 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 other words, interests that are too vague or speculative are not enough. If the legitimate interests are not formulated clearly enough, it is not possible to balance said interests with the interests and fundamental rights of the data subject. Therefore, it is important that the legitimate interest is in accordance with the current legislation, formulated clearly enough (ie sufficiently specific) and real and present at the moment (ie not speculative). Secondly, it is necessary to analyze what are the possible interests or fundamental rights of the data subject - and the freedoms that may be harmed by the processing of personal data. Third, the legitimate interests of XXX must be balanced with the interests and fundamental rights of the data subject. In doing so, the impact that may arise on the data subject from the processing (collection, use, storage) of personal data is compared with the legitimate interests of the controller, and it is assessed whether and to what extent the legitimate interest of the controller outweighs the interests of the data subject. We emphasize 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 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. 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 familiarize himself with it at any time (see IKÜM Article 13(1)(d)). 3. Drafting of data protection conditions Data processing must be transparent. The principle of transparency requires that all information and messages related to the processing of personal data are easily accessible, understandable and clearly worded. In other words, data protection conditions must be drawn up. The content of the data protection conditions is regulated by articles 12 - 14 of the IKÜM. Hereby, we emphasize that all information provided in articles 13 -14 of the IKÜM must be regulated in the data protection conditions. If any of the provisions of the above articles remain unclear, we recommend that you also familiarize yourself with the guidelines of the Article 29 working group on transparency3, where the content of the points stipulated in

Articles 13 - 14 of IKÜM is explained in more detail on pages 35 - 40. Here we explain that every personal data processor must have data protection conditions that regulate the activities of a specific personal data processor. At the same time, the conditions for the use of cameras must also be regulated. In a situation where cameras are used, the data protection conditions or camera procedures 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. Article 13 of the IKÜM stipulates that the data controller shall inform the person of all the information stipulated 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 and contact details of the data controller, and information where the data protection conditions can be found. easily available. 3. -to the organizer/is-your-video-surveillance-nouab-notification label 4. Storage period of the camera recording The European Data Protection Board has outlined the following in its guidelines 3/2019 on the processing of personal data in video devices:5"Taking into account the principles set forth in Article 5(1) points c and e of the General Regulation on the Protection of Personal Data , namely the collection and retention of as little data as possible, personal data should in most cases (e.g. to detect vandalism) 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. We also emphasize here that the longer the recordings are stored, the greater the impact is on the persons who were left on the recordings. In order to be able to check in retrospect

who, when and which camera 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. 5. Compliance with IKÜM requirements There is no legal basis for filming properties belonging to other persons that would allow them to infringe on their right to privacy. However, depending on the situation, it may be justified to film a public area. Since XXX has not submitted to AKI a mandatory legitimate interest analysis for the use of cameras and filming of public areas, the use of cameras is not permitted based on Article 6(1)(f) of the IKÜM, and the cameras must be removed until a correct legitimate interest analysis has been prepared regarding the use of cameras, which it becomes clear whether and to what extent (e.g. in which places more precisely) cameras can be used. In case of redirection of cameras, photos of the camera image must be provided so that the inspection can check its scope. We explain that video surveillance in an area, which partially also includes a public area, could theoretically be used only if a correct legitimate interest analysis is prepared and it shows that your legitimate interests outweigh the interests of the data subjects. You have not prepared such an analysis. Therefore, if you still want to use video surveillance in your territory, you must prepare a correct legitimate interest analysis that meets the conditions set forth in Article 6(1)(f) of the IKÜM (see point 2 of the inspection's reasons). In addition, proper notification signs about the use of video surveillance must be created and installed, and photos of the installed signs must be submitted to the inspection, and data protection conditions must be drawn up and forwarded to the inspection, which fully meet the requirements set forth in Articles 12 and 13 of the IKÜM (see point 3 of the inspection's reasons). Summary: 1. XXX must stop filming outside his own property (either by dismantling the camera(s) or directing it so that only his own property remains), 2. XXX must delete the existing recordings and send confirmation of this to the inspection at info@aki.ee ; 3. If the cameras are redirected, send photos of the camera image to the Data Protection Inspectorate at the e-mail address info@aki.ee to check its scope; 5. which meets the conditions set forth in point f of Article 6, paragraph 1 of the IKÜM (see point 2 of the inspection's reasons). We emphasize that the analysis of the legitimate interest must be so clear that it is possible to understand why the processor actually uses the cameras and what he has done so that the rights of the data subjects are not excessively harmed; 5. In the event that XXX wishes to use video surveillance, proper notification signs about the use of video surveillance must be created and installed, and photos of the installed signs must be submitted to the inspection (see point 3 of the inspection's reasons); 6. If XXX uses video surveillance, a confirmation must be sent to the inspection that the video recordings will be deleted immediately, but at the latest after 72 hours (see point 4 of the inspection's

reasons). A longer storage period is allowed if XXX justifies the need for a longer storage period and the inspection gives a corresponding confirmation; 7. In the event that XXX uses video surveillance, data protection conditions must be drawn up and submitted to the inspectorate, which fully meet the requirements set forth in Articles 12 and 13 of the IKÜM (see points 3 of the inspection's reasons). (digitally signed) Alissa Khmelnitskaja lawyer under the authority of the Director General