FOR 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.-5/23/2962 Prescription issued by Data Protection Inspectorate lawyer Jekaterina Aader Time and place of making the injunction 13.04.2023 in Tallinn Recipient of the injunction - personal data processor Roval Agro OÜ, registry code 12908851 address: Saare county, Saaremaa parish, Kuressaare city, Nooruse tn 45, 93816 e-mail address: roland@roval.ee Personal data processor responsible person Board members RESOLUTION: § 56 (1), (2) point 8, § 58 (1) of the Personal Data Protection Act (IPS) and Article 58 (2) points a and f, Article 5 (1) point a, Article 6 of the General Regulation on Personal Data Protection (IKÜM) on the basis of point f of paragraph 1, I issue a mandatory injunction for compliance: 1. stop processing (filming) personal data with the camera outside the property belonging to Roval Agro OÜ (neighboring properties, public area), either by changing the camera's filming angle or by repositioning the camera so that nothing remains in the camera's field of view other than the property belonging to the company and send screenshots of the camera image to the e-mail address info@aki.ee to prove it. 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 27.04.2023. 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 16.12.2022, the Data Protection Inspectorate received a complaint regarding a surveillance camera installed at the intersection of the Kurevere-Harila-Harilaiu road and the road passing through the Ees-Kordon land unit in Kõrus village, Saaremaa municipality, Saare county, with a filming trajectory perpendicular to the Kurevere-Harila-Harilaiu road. According to the complainant, there is no information about the camera owner, the purpose of video data collection and storage at the location of the camera, and there is only a yellow sign near the camera informing about video surveillance. According to the applicant, the camera monitors the movement of his family and guests to the Saariste-Sandri land unit and thereby invades his privacy. Attached to the complaint are photos confirming the complainant's words and a plan with the coordinates of the camera's location. On 06.02.2023, the inspection found out that the publicly used Kurevere-Harila-Harilaiu municipal road perpendicular to the direction of the surveillance camera is located on the Ees-Kordon land unit (cadastral code 71401:001:1094) belonging to Roval Agro OÜ (registration code 12908851). On 10.02.2023, the inspection sent an inquiry to the camera owner (data processor) for clarification and a proposal to change the camera's filming angle so that nothing remains in the camera's field of view except the property belonging to Roval Agro OÜ (neighboring properties, public area) and to send screenshots of the camera image to prove this, delete the existing recordings and submit a confirmation of the filled-in. 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 inquiry, the inspectorate explained the legal basis and conditions for filming a public area or neighboring properties with a camera. The inspection set 22.02.2023 as the deadline for completing the proposal. On 13.02.2023, the data processor sent an e-mail in response to the inquiry and proposal, in which he explained the purpose of using the video camera and filming the public area, which was the protection of property, and presented a diagram of the location of the camera and the filming angle. In the answer, the data processor also explained the location of the public area, neighboring and own properties and their use. The data processor did not respond to the inspection's inquiry about the legal basis of the filming and the place and term of storage of the recordings, nor has it forwarded to the inspection any photos of the camera image where an object (e.g. a vehicle) or a person has been captured. As a solution to the situation, the data processor offered to change the location of the camera and relocate it closer to the neighboring property (behind the gate of the Saariste property) facing its own land so that no public area is filmed. On 23.02.2023, the inspectorate sent an additional

proposal to change the camera's filming angle so that nothing but the property belonging to the company remains in the camera's field of view and to send screenshots of the camera image to prove this, to stop recording sound with the camera, to delete the existing recordings and to submit a confirmation of the completed action. As an alternative demand, the inspectorate again 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. The inspection set 10.03.2023 as the deadline for completing the proposal. However, the data processor has not responded to the inspection's proposal. On 04/05/2023, the inspectorate sent a reminder by e-mail about the failure to respond to the proposal and requested information on whether the company has relocated the camera or changed the camera's field of view. The inspection gave time until 10.04.2023 at the latest to respond, warning that an injunction may be issued to the company if it is not answered. The company has not responded to the reminder either, therefore issuing an injunction is inevitable PERSONAL DATA PROCESSOR'S EXPLANATION: The data processor essentially failed to respond to the inspection's inquiries and proposals, explaining only the purpose of using the video camera and filming the public area, which was property protection. The data processor did not explain the legal basis for the use of stationary cameras, the purpose of filming, necessity, scope, conditions of data processing and other circumstances. The data processor has not responded to both proposals of the inspection or confirmed their implementation. 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 does not apply to legal entities, therefore the inspection does not consider this issue within the scope of this prescription. 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.1 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, there must be a real situation, for example previous damage or previous serious incidents.2 1 Opinion 06/2014 on the concept of legitimate interests of the data controller in the sense of Article 7 of Directive 95/46/EC. 2 Guidelines of the European Data Protection Board 3/2019 on the processing of personal data in video devices (Guidelines for Video Surveillance), page 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. In general, the need to use video surveillance to protect the property of the data controller ends at the borders of the property.3 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 hand.4 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)5. 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 camera installed at the intersection of the Kurevere-Harila-Harilaiu road and the road passing through the Ees-Kordon land unit in Kõrus village, Saaremaa municipality, Saare County, as a result of which the use of cameras filming the public area is not permitted under Article 6(1)(f) of the IKÜM allowed. Therefore, the use of cameras must be stopped until a correct legitimate interest analysis has been prepared regarding the filming of a public area, from which it becomes clear 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. 3 Video surveillance guidelines, p. 10-11, p 24-27. 4 Video surveillance guidelines, p. 11, p. 30. 5 IKYM art. 5 paragraph 2 and art. 12-14, see also justification point 76. The camera notification sign should be placed so that it is easy for a person to become aware of the camera surveillance before entering the monitored area. 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 assess which area is in the camera's field of view, so that he can avoid surveillance or adjust his behavior if necessary.6 8. One of the criteria for the legality of personal data processing in Article 5(1)(a) of IKÜM is to ensure the transparency of data processing, namely that all personal data related to processing must information and messages should 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 conditions7. 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. 9. It can be seen from the image material that there is a yellow sign informing about video surveillance without any information at the camera installed at the intersection of the Kurevere-Harila-Harilaiu road and the road passing through the Ees-Kordon land unit in Kõrus village, Saaremaa municipality, Saare county. However, the label "Video surveillance" alone does not convey all the necessary information about the data processor and the conditions of data processing. In this case, the persons who remain in the field of view of the camera do not have information about whom they must turn to and under what conditions they will be recorded on the camera image. Thus, the camera owner failed to fulfill the notification obligation of the data processor. Retention of camera recording 10. In accordance with Article 5(1)(c) and (e) of the IKÜM, personal data may not be retained 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:8 "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 data controller is responsible for determining the retention period in accordance with the principle of necessity and proportionality and compliance with the provisions of the General Data Protection Regulation. 8 Video surveillance guidelines, p. 28, p. 121. for proof. 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. 11. Article 32, paragraph 1 of IKYM 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.9 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. 12. 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.10 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). Summary 13. As a result of the above, in order to be able to use video surveillance outside their property and monitor public spaces with cameras, the data processor must fulfill the following requirements: 1) prepare a correct legitimate interest analysis that meets the conditions set forth in point f of Article 6(1) of the IKÜM (see the points of the inspection's reasons 4-5); 2) create and install appropriate information signs11 about the use of video surveillance (see point 7 of the inspection's reasons); 3) prepare data protection conditions that fully comply with the requirements stipulated in Articles 12 and 13 of the IKÜM (see point 8 of the inspection's reasons) 4) ensure that the video recordings are deleted immediately, but no later than after 72 hours (see point 10 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 a public area. According to the inspection, the data processor must therefore stop any filming of public areas with cameras without a legal basis and delete all existing recordings. This does not exclude the possibility of using the cameras to film a public area, if the data processor has submitted a proper legitimate interest analysis and fulfilled the notification obligation. (digitally signed) Jekaterina Aader lawyer under the authority of the director general 9 Videovalve guidelines, page 28, p 123. 10 IKÜM article 15.11 The notification label can be created using the AKI label generator at the web address videovalvesilt.aki.ee.