FOR PRIVACY PROTECTION AND STATE TRANSPARENCY Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 PRELIMINARY WARNING in personal data protection case no. 2.1.-5/22/1340 Injunction maker Alissa Jarova, lawyer of the Data Protection Inspectorate Time and place of injunction 12.08.2022 in Tallinn Addressee of injunction - personal data processor LUX-MEDICUS Finland OÜ (12048851) mikhail.kordas@mail.ru; meditsiin@mail.ru Responsible official of the personal data processor Member of the Board RESOLUTION: Clause 56 (1) and (2) point 8, § 58 (1) of the Personal Data Protection Act (hereinafter IKS) and Article 58 (1) point d and paragraph 2 of the General Regulation on Personal Data Protection (hereinafter IKYM) points d, e and f, as well as taking into account articles 5, 6, 12 and 13 of IKÜM, the Data Protection Inspectorate issues a mandatory order for LUX-MEDICUS Finland OÜ to comply with: 1. Remove audio surveillance from all premises of LUX-MEDICUS Finland OÜ (see points 2 and 3.1); 2. Remove video surveillance from all premises of LUX-MEDICUS Finland OÜ until a correct legitimate interest analysis has been prepared regarding the use of cameras, which will reveal whether and to what extent (e.g. in which places more precisely) cameras may be used (see points 2 and 3.1 of the inspection's reasons); 3. Notify employees of a violation related to the use of video surveillance (with audio recording) (see point 3.3 of the inspection's reasons). Send the inspection a copy of the letter that was sent to the employees regarding the violation; We set the deadline for the execution of the order to be 31.08.2022. 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 Administrative Court Procedure Code 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 2 (9) imposes an extortion fee of 5,000 euros on 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 (1) of the Personal Data Protection General Regulation may result in a misdemeanor proceeding based on § 70 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 (hereinafter AKI) received a tip that surveillance devices - (security) cameras are used in the beauty clinic offices of LUX-MEDICUS Finland OÜ. Therefore, AKI has started a monitoring procedure on the basis of IKS § 56 (3) point 8, within the framework of which we wanted to know, among other things, the following: 1. Where and in which rooms has LuxMedicus OÜ installed surveillance cameras? Please provide a diagram of the location of the cameras and a more detailed description of which cameras you use. Including whether they can be zoomed, rotated, record sound, etc. 2. For what purpose are the cameras installed? Will and when will the employees' performance of duties and customers be monitored via cameras? 3. We ask you to provide the analysis of the legitimate interest assessment carried out before using the cameras; 4. Are and how have the data protection conditions created on the basis of articles 12-13 of the IKÜM regarding the use of video cameras been communicated to individuals (customers and employees)? For this purpose, we ask you to send a copy of the rules of work organization, etc. of the document with which the employees of the institution have been informed and a reference to the data protection conditions on the company's website (or, in the case stipulated in the customer contract, an extract). 5. Explain who has access to the recordings, including in which cases the recordings can be viewed and what security measures are implemented to prevent access by unauthorized persons. Including what kind of logs are created every time you log into the system and watch the recordings, and can you distinguish who has been watching the recordings? Please provide a sample of the last month's viewing logs. On 22.07.2022, the representative of LUX-MEDICUS Finland OÜ sent a reply, which revealed that the company has not prepared a legitimate interest analysis for the use of video cameras (with audio recording), there are no data protection conditions and correct information labels about the use of cameras. 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). With the help of cameras, a person (especially an employee) can be identified in any case. LUX-MEDICUS Finland OÜ also stated that both surveillance cameras have audio recording (located in the reception room 3 (9) and the procedure room). The voice is also a personal gift, by which it is possible to identify a person. In the case of video and audio surveillance (audio recordings), it is a matter of personal data processing, which must comply with the requirements stipulated in the IKÜM. 2. Principles of personal data processing 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: - Legality, fairness and transparency (IKÜM Article 5(1)(a)) Any processing of personal data must be fair and legal, i.e. fully in accordance with all applicable 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 state what the 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. Collection of as little data as possible (IKÜM Article 5(1) points b, c and e) In order to assess whether the use of cameras complies with the principle of goal limitation and 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 objectives or whether there are other measures that are less intrusive to the data subject. It is forbidden to monitor employees with cameras during the entire working time, and the cameras must be directed to specific security risks. The processing of personal data must be stopped and the data must be deleted or transferred to a non-personalized form as soon as the legal basis ceases and/or the purposes for which they were collected have been fulfilled. The time for processing personal data must be strictly limited to the minimum. In order to ensure that personal data is not processed longer than necessary, the controller must determine the deadlines for deleting personal data and for periodic review. Regarding the storage of camera recordings, we note the following. In its guidelines 3/2019 on the processing of personal data in video devices, the European Data Protection Board has stated the following:1 "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 for the purpose 1

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_et.pdf page 28 p 121 4 (9) actually necessary to achieve. 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. Here, we also emphasize that the longer the recordings are stored, the greater the interference is for the persons left on the recordings (including employees, customers). - 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) In order to be able to check 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. 2.1. 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. According to the inspection, the legal basis for the use of cameras at LUX-MEDICUS Finland OÜ could be derived from IKÜ Article 6(1)(f). 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 basis of 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 also 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, LUX-MEDICUS Finland OÜ must prove whether and what the legitimate interest of the company is and that it outweighs the rights of individuals. 5 (9) 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. Thirdly, the legitimate interests of LUX-MEDICUS Finland OÜ must be balanced with the interests and fundamental rights of the data subject. In doing so, the possible impact 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 legitimate interest must be documented and it must be possible for any person (including an employee) to consult it at any time (see IKÜM Article 13(1)(d)). Although it is generally sufficient if the data protection conditions only indicate how it is possible to read the analysis of legitimate interest (e.g. to read the analysis, write to the e-mail address info@bestablanimi.ee), in the case of cameras used in the workplace, this is a very intrusive measure, and for that, so that the legitimate interests of the data processor outweigh the interests of the employees, the greatest possible transparency must also be ensured, including

enabling easy access to the analysis of the legitimate interest (e.g. in the rest room). It must also be taken into account that the employee is, as a rule, the weaker party in the employment relationship, and a situation may arise where the employee does not dare to ask for a legitimate interest analysis in writing. 2.2 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 transparency2, where the content of the points stipulated in Articles 13 - 14 of IKÜM is also explained in more detail on pages 35 - 40. Here we explain that every processor of personal data 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. 2. among others, the following: - 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 informs 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. In addition, we explain that the analysis of legitimate interest must be included in the data protection conditions or the analysis of legitimate interest must be prepared as a separate document and made easily available at the workplace (e.g. in the break room). 3. Compliance with all requirements 3.1 LUX-MEDICUS Finland OÜ's legal basis for using video and audio surveillance We explain that video and audio surveillance could theoretically be used only if a correct legitimate interest analysis has been prepared and it can be seen that the legitimate interests of the company outweigh the data subject interests. Such an analysis has not been prepared by LUX-MEDICUS Finland OÜ. The use of audio monitoring could be justified only by very exceptional circumstances, which,

according to the inspection, do not exist for the data processor. The European Data Protection Inspector has already stated in 2010 that the use of audio recordings in the workplace is prohibited.3 This is also confirmed in the guidelines of the European Data Protection Board, which states that monitoring devices should not offer functions that are not necessary (e.g. audio recordings). Therefore, in any case, unnecessary functions must be deactivated or surveillance devices with no additional functions must be introduced.4 The permissibility of using audio surveillance for the purpose of ensuring security, resolving customer disputes, detecting possible fraud, etc. can lead to the same extensive practice as video surveillance is already used. At the same time, for the most part, all the conditions that would allow this have not been met. Video surveillance has not always been the normality of everyday life either. Over time, video surveillance is exploited more and more, while the functionalities and quality of video surveillance improve. Over time, people have accepted the inevitability of video surveillance being used on such a large scale. By starting to use audio surveillance for the same purposes, step by step at first in some companies, it spreads indiscriminately everywhere and it is in no way acceptable based on the very important invasion of privacy. 3 European Data Protection Supervisor, Video-surveillance Guidelines, 2010, p 6.12 - https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf 4 European Data Protection Board, Guidelines 3/ 2019 on the processing of personal data in video devices, 2020, point 129 - https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_et.pdf 7 (9) Since LUX-MEDICUS Finland OÜ has left a mandatory legal basis for the use of cameras without preparing an analysis of interest, the use of cameras is not permitted on the basis of 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 revealed whether and to what extent (e.g. in which places more precisely) cameras can be used. Since the use of audio surveillance at the workplace is prohibited and LUX-MEDICUS Finland OÜ has not cited exceptional circumstances, due to which it would still be necessary to use audio recordings at the workplace, the inspection is of the opinion that audio surveillance is not allowed in the premises of LUX-MEDICUS Finland OÜ under any circumstances due to the IKÜM. 3.2 Time limit for storing video recordings LUX-MEDICUS Finland OÜ stated that the company's privacy policy states that "audio and video recording is carried out in the clinic to protect the rights of the patient and the clinic staff. The recording is stored on the hard drive for up to 30 days. Pubic care procedures are carried out in the office without sound and video cameras. "First of all, LUX-MEDICUS Finland OÜ has not explained why it is necessary to store camera recordings for up to 30 days, and secondly, it is a very long storage period. The

longer the retention period, the greater the burden on data subjects, especially employees, because longer time means more data. Since LUX-MEDICUS Finland OÜ has not justified the necessity of the storage period for the camera recordings, and the inspection does not see that such a long storage period can be legitimate, LUX-MEDICUS Finland OÜ must in the future delete the recordings immediately, but no later than after 72 hours. In the opinion of the inspectorate, in order to protect the rights of employees, it is necessary to establish a restriction on the processing of personal data (limit the period of storage of video recordings) until LUX-MEDICUS Finland OÜ has proved to the inspectorate that the storage of video recordings for longer than 72 hours actually complies with the principles of personal data processing (see IKÜM article 5 paragraph 1 points b, c and e) and the inspection has confirmed the legality of the longer storage period. 3.3 Notifying employees of the violation The use of both video and audio surveillance represents a very intense invasion of privacy, therefore it is particularly important that in a situation where video and audio surveillance have been installed illegally, i.e. the installation did not and does not comply with the principle of personal data processing (principle of legality), video- and the audio surveillance will be removed immediately, and the employees will also be informed of the violation (see IKÜM Article 34 paragraph 1). The breach notification describes in clear and simple language the nature of the breach related to personal data and provides at least the following information (see Articles 34 paragraph 2 and 33 paragraph 3 of IKÜM): 1. Name and contact details of the contact person, through which it is possible to obtain more detailed information about the breach; 2. Describe the possible consequences of a breach of personal data; 3. Describe the measures taken or planned to be taken to resolve the personal data breach. Therefore, LUX-MEDICUS Finland OÜ must convey the above information to the employees and confirm to the employees that the video and audio surveillance has been removed. 3.4 Notification signs 8 (9) LUX-MEDICUS Finland OÜ provided the Inspectorate with photos showing that some signs about the use of video surveillance have been installed in the clinic, but these signs do not meet the requirements. The notification label must have the following information: - purpose of processing; - legal basis; - the name and contact details of the data controller; - information where you can get acquainted with the data protection conditions. As a result, LUX-MEDICUS Finland OÜ must create and install proper information signs about the use of video surveillance. 3.5 LUX-MEDICUS Finland OÜ data protection conditions In its response to the inquiry, LUX-MEDICUS Finland OÜ referred to the privacy policy document, which states that "the processing of personal data at the Lux-Medicus beauty clinic takes place on the basis of the law and in accordance with the data protection regulations and the clinic's privacy policy. We explain that the form of the mentioned document is not correct data protection conditions, as the

content of the document is not based on article 13 of IKÜM (see also section 2.2 of the inspection's reasons for the mandatory content). Based on the above, this document does not meet the requirements stipulated in IKÜM (IKÜM article 5 paragraph 1 point a, article 12 paragraph 1 and article 13 paragraphs 1 and 2). Summary: 1. LUX-MEDICUS Finland OÜ has no legal basis (legitimate interest) for using video and audio surveillance, and the video and audio surveillance must be removed immediately. Since video and audio surveillance have been used illegally, employees must be informed of the violation; 2. In order to use video surveillance, a correct legitimate interest analysis must be prepared that meets the conditions set forth in Article 6(1)(f) 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 the employee can understand why the employer actually uses cameras and what he has done to ensure that the employee's rights are not excessively harmed; 3. In the event that LUX-MEDICUS Finland OÜ still wants to use video surveillance on its territory, it is necessary to create and install proper notification signs about the use of video surveillance and submit photos of the installed signs to the inspection (see points 2.2 and 3.4 of the inspection's reasons); 4. In the event that LUX-MEDICUS Finland OÜ decides to use 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 points 2 and 3.2 of the inspection's reasons). A longer storage period is allowed if LUX-MEDICUS Finland OÜ justifies the need for a longer storage period and the inspection gives a corresponding confirmation; 5. In the event that LUX-MEDICUS Finland OÜ uses video surveillance, data protection conditions must be prepared and forwarded to AKI, which fully meet the requirements set forth in Articles 12 and 13 of IKÜM (see points 2.2 and 3.5 of the inspection's reasons). Given that the use of video surveillance in LUX-MEDICUS Finland OÜ is not legal (there is no analysis of legitimate interest), a correct analysis of legitimate interest must be submitted to the inspection by the deadline, or the cameras must be removed and a corresponding confirmation sent. 9 (9) In accordance with § 58 subsection 1 of the Personal Data Protection Act and Article 58 subsection 2 points d, e and f of the General Regulation on Personal Data Protection, the inspectorate has the right to establish a temporary or permanent restriction on the processing of personal data, including a processing ban, and to order that: - the responsible processor personal data processing operations in a certain way and within a certain period of time to comply with the requirements of the IKÜM; - the data controller would inform the data subject of a violation related to his personal data. Taking into account the factual circumstances and the fact that in a specific case personal data is processed illegally (data processing does not meet the requirements set forth in Articles 5, 6, 12 and 13 of the IKÜM), the inspection considers that issuing a mandatory injunction in this case is necessary to end the

offense as soon as possible and ensure the protection of the rights of employees. (digitally signed) Alissa Jarova lawyer under the authority of the General Director