Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 PRELIMINARY WARNING in personal data protection case no. 2.1.-1/21/3828 Issuer of the injunction Data Protection Inspectorate lawyer Mehis Lõhmus Time and place of issuing the injunction January 21, 2022 Tallinn Recipient of the injunction - personal data processor Nerostein OÜ address: e-mail address: indrek@nerostein.com Responsible official of the personal data processor Nerostein OÜ board member RESOLUTION: § 56 (1), (2) point 8, § 58 (1) of the Personal Data Protection Act (IPS) and Article 58 (1) points a and d and (2) points c and d of the General Regulation on Personal Data Protection (IKÜM), also considering the IKÜM with articles 5, 6, 7, 12, 13, 14, 15 and 32 paragraph 1, the Data Protection Inspectorate issues a mandatory injunction to Nerostein OÜ to comply with: 1. Answer the questions sent by Xi on November 9 and 10, 2021 (a) "I would like to know how and how did you observe my work? ", b) "Please also the section of the law, on the basis of which you monitored my work without informing me about it? ") stating which Xi's personal data was used by Nerostein OÜ to monitor him, in which way the personal data was collected for this purpose and on which legal basis (refer to the specific IKÜM article) this was done. 2. Send a copy of the answer to the e-mail address of the Data Protection Inspectorate at info@aki.ee. 3. Create data protection conditions of Nerostein OÜ that correspond to Articles 12-14 of the General Regulation on Personal Data Protection and publish them on Nerostein OÜ's website www.nerostein.ee. The data protection conditions must, among other things, be easily found (presumably in the footer of the page). 4. Create a proper cookie consent form on the Nerostein OÜ website www.nerostein.ee. 5. Make data processing on Nerostein OÜ's website www.nerostein.ee secure. For this purpose 2 (8) Nerostein OÜ must add a certificate on its website. Currently the web page is HTTP, but for data processing it must be HTTPS. We set the deadline for the fulfillment of the injunction to be February 4, 2022. Report the fulfillment of the injunction to the Data Protection Inspectorate's e-mail address info@aki.ee by this deadline at the latest. REFERENCE FOR DISPUTES: You can contest this order within 30 days by submitting either: - an appeal in accordance with the Administrative Procedure Act to the Data Protection Inspectorate or - an appeal in accordance with the Administrative Court Procedure Code to the Tallinn 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 issue the addressee of the injunction on the basis of § 60 of the Personal Data Protection Act: Extortion money of 5,000 euros for each unfulfilled injunction point. 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: On November 23, 2021, the Data Protection Inspectorate received a complaint from X (X@gmail.com) regarding the fact that Nerostein OÜ has not responded to the data subject's request. On November 24, 2021, the Data Protection Inspectorate failed to start the procedure, explaining the following to the applicant: "According to Article 12, Paragraph 3 and Article 15 of the General Regulation on Personal Data Protection, a person has the right to receive information about the processing of his data within one month of submitting the request at the latest. The information that a person has the right to receive also includes the documents related to him, in this case the documents that are the basis of the monitoring. The correspondence sent to us shows that you sent your request on November 10, which means that Nerostein OÜ still has time to respond to your request. Since it is not possible to come to the conclusion based on the submitted complaint that the requirements of the Personal Data Protection Act have been violated by monitoring the work processes of 3 (8) employees, I will not initiate the procedure. However, the above does not prevent you from submitting a new proper complaint with documents proving the violation (e.g. in a situation where it has been made clear that there was no basis for the monitoring or the data processor fails to respond on time). Since Nerostein OÜ had not responded to the complainant on time, X submitted a new complaint to the Data Protection Inspectorate on January 4, 2022. On January 4, 2022, the Data Protection Inspectorate forwarded the applicant's questions with a cover letter to Nerostein OÜ to answer, with the wish to avoid administrative burden and not to start a supervisory procedure, hoping that the matter will be resolved simply by answering the inquiry. Among other things, Andmekaitse Inspektsioon Nerostein OÜ drew attention to the fact that they do not have data protection conditions and visitors to the website www.nerostein.ee are not asked for their consent to use cookies. The Data Protection Inspectorate asked to eliminate the deficiencies by January 20, 2022 at the latest and to answer the complainant's questions by January 11, 2022 at the latest. Nerostein OÜ responded to the Data Protection Inspectorate on January 5 and explained the following: "I explain that the employment relationship with the petitioner was terminated during the probationary period, and the reasons for the termination

were also explained to the employee when the notice of termination was handed over. Indeed, it was described that the employer monitored the employee during the probationary period, meaning the usual control of the employee's performance and the compliance of the employee's behavior and personality to work in the given workplace. As stated above, after sending a letter to AKI, the meaning and content of which, unfortunately, Nerosten did not understand, and the contents of which we still had a dispute within the organization, we soon received an invitation to the session of the Labor Disputes Committee, where the substantive dispute regarding the termination of the employment contract will also take place. The employee himself forwarded the employment contract, the job description directly to TVK. The employee should have access to the employee register, i.e. the corresponding register always sends a notification of the corresponding entries to the employee as well. I would like a more detailed explanation from AKI, what information regarding the monitoring of the employee, according to your institution, must be submitted to the petitioner? In addition, is it legal to deal with the subject of "monitoring" at this moment in a situation where there is an ongoing labor dispute? In the case of specific requests of employees regarding certain documents, we are ready to submit them to the employee if they do not concern the ongoing labor dispute. If the document concerns a labor dispute, according to the law, TVK requires Nerostein to submit it. We ask for specific explanations and further instructions, because at the moment, unfortunately, Nerostein inevitably has the impression that the employee, either intentionally or by mistake, has given a completely different content to the usual monitoring of employees during the probationary period in his letter, which he forwarded to me and AKI, and is currently wasting both AKI's and Nerostein's resources without justification. The Data Protection Inspectorate explained to Nerostein OÜ on January 7, 2022 that responding to the data subject's request does not interfere with the ongoing labor dispute. The data subject has asked specific questions about the processing of his personal data. Monitoring is also the processing of personal data (be it monitoring from a camera, evaluating work processes on a computer or another way of monitoring). We explained that on the basis of Article 12 (3) of the General Regulation on the Protection of Personal Data, the data controller shall provide the data subject without undue delay, but no later than within one month after receiving the 4 (8) request, information on the measures taken on the basis of the request in accordance with Articles 15-22. The data subject submitted his questions on November 9 and 10, 2021. The data subject's request clearly corresponded to the provisions of Article 15 of the General Regulation on the Protection of Personal Data. We reminded, among other things, in the explanation sent on January 7, 2022, that Nerostein OÜ must add proper data protection conditions to its website, corresponding to Articles 12-14 of the General Regulation on the Protection of

Personal Data, and ask for the consent of website visitors for the use of cookies. On January 11, 2022, despite the explanations of the Data Protection Inspectorate, you responded to Xi's letter as follows: "The content of your letter is incomprehensible to Nerostein. If you have a claim against Nerostein, it is currently unclear. In addition, the claim has not been submitted to the correct person. Based on the above, please submit a clear claim to the company's legal representative (CEO Indrek Vallaste). When submitting a claim, state the object and the basis. "The Data Protection Inspectorate had explained to you the reasons behind the complainant's questions and their content. Therefore, there was no reason to send the above letter to the applicant. On January 17, 2022, the applicant sent a notification to the Data Protection Inspectorate that his questions were not answered. Among other things, as of January 21, 2022, Nerostein OÜ has not eliminated the deficiencies pointed out by the Data Protection Inspectorate (data protection conditions and asking for cookie consent). Insofar as Nerostein OÜ had not answered the complainant's questions in substance and the indicated deficiencies had not been eliminated by the prescribed deadline, the Data Protection Inspectorate started the supervisory procedure on the basis of § 56 subsection 3 point 8 of the Personal Data Protection Act. When starting the procedure, the Data Protection Inspectorate discovered another deficiency in the data processing of Nerostein OÜ, which was not previously brought to attention. Namely, the data processing on the website of Nerostein OÜ is insecure. More on this in the reasons of the Data Protection Inspectorate below. PERSONAL DATA PROCESSOR'S EXPLANATION: The addressee of the injunction has been given a reasonable deadline to answer the complainant's questions. Among other things, the Data Protection Inspectorate explained the reasons behind the complainant's questions and their content. In addition, Andmekaitse Inspektsioon Nerostein OÜ drew attention to the shortcomings on their website, where there were no data protection conditions and website visitors were not asked for their consent to collect cookies. The Data Protection Inspectorate gave Nerostein OÜ reasonable deadlines to respond to the complainant and to eliminate deficiencies on the website. Nerostein OÜ was supposed to respond to the complainant by January 11, 2021, but the complainant's questions were answered as incomprehensible. Nerostein OÜ had to eliminate the shortcomings pointed out by the Data Protection Inspectorate no later than January 20, 2022. This is enough time to ask the Data Protection Inspectorate for 5 (8) additional explanations if necessary. Unfortunately, as of January 21, 2022, Nerostein OÜ has not eliminated the deficiencies, nor has it expressed its opinion about them. GROUNDS FOR THE DATA PROTECTION INSPECTION: Responding to the data subject's request Article 15 of the General Regulation on the Protection of Personal Data (GPR) states that the data subject has the right to receive confirmation from the data controller as to whether

personal data concerning him/her is being processed, and in such a case to consult the personal data and, among other things, the following information: a) the purpose of the processing; b) the types of personal data concerned; and c) if the personal data is not collected from the data subject, the available information about its source. The complainant sent you the following questions: 1) "How and in what way did you observe my work?" " 2) "Please also the section of the law under which you monitored my work without notifying me? According to IKÜM art 15, to answer these questions, it is necessary to explain which personal data of the data subject (i.e. Xi) was used by Nerostein OÜ to monitor the data subject, in what way the personal data was collected for this purpose and on what legal basis (i.e. refer to a specific article of IKÜM). In this case, Nerostein OÜ failed to fully respond to the data subject's request (questions). After explanations from the Data Protection Inspectorate, the complainant was told that the questions were incomprehensible, regardless of the fact that the Data Protection Inspectorate explained the basis of the questions. On the basis of Article 12(3) of the General Regulation on the Protection of Personal Data, the data controller shall provide the data subject with information on the measures taken on the basis of the request in accordance with Articles 15-22 without undue delay, but no later than one month after receiving the request. The data subject submitted his questions on November 9 and 10, 2021, and as of January 7, 2022, they were clearly exceeded, which is why Nerostein OÜ has violated the obligation arising from the General Regulation on Personal Data Protection. Data protection conditions Nerostein OÜ's website www.nerostein.ee does not have data protection conditions in accordance with Articles 12-14 of the General Regulation on Personal Data Protection. We repeatedly explained to Nerostein OÜ that they must have data protection conditions. Article 5(1)(a) of the General Regulation on Personal Data Protection stipulates the principle of transparency. 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 6 (8) data protection conditions. Among other things, we explained that if any of the provisions of the aforementioned articles remain unclear, it is reasonable to consult the guidelines of the Article 29 working group on transparency1, where the contents of the points stipulated in Articles 13 - 14 of the IKÜM are also explained in more detail on pages 35 - 40. We added that each personal data processor must have data protection conditions that regulate the activities of a specific personal data processor. The data protection conditions must be concise, clear and understandable and meet the conditions set out in the General Regulation on

Personal Data Protection. Here, it must be taken into account that the controller must present the information in such a way that a person can clearly understand it and that it is distinguished from information that is not related to the controller's personal data processing. It is crucial to understand that data protection conditions are not created simply to get a checkmark, but must be based on the data processing of the data controller, which assumes that the data processing is precisely mapped and understandable to the drafter of the data protection conditions. To the extent that Nerostein OÜ has not yet added the proper data protection conditions to its website, an injunction is necessary. Cookie consent Nerostein OÜ's website www.nerostein.ee collects various cookies, including Google Analytics cookies, but visitors to the website are not correctly asked for their consent to the collection of cookies. Article 6 point a of the General Regulation on the Protection of Personal Data states that the processing of personal data is legal only if the data subject has given consent to process his personal data for one or more specific purposes. Paragraph 30 of the preamble of the General Regulation on the Protection of Personal Data states that natural persons may be associated with network identifiers shared by their devices, applications, tools and protocols, such as IP addresses or cookies, or with other identifiers, such as radio frequency identification chips. This may leave traces that may be used to profile and identify natural persons, in particular when combined with unique identifiers and other information arriving at the servers. Therefore, the collection of cookies is clearly the processing of personal data, and for this Nerostein OÜ needs a legal basis arising from the law, which can only be the consent of the data subject in established practice in Europe. We clarify that according to the Directive on privacy and electronic communications, users should be able to prevent the storage of cookies or other such means on their end device. Information about the means stored on the user's different end devices and the right to refuse them may be provided once during one and the same connection, and may also include the future use of said means during subsequent connections. Providing information, offering the option to refuse or asking for consent should be made as user-friendly as possible. Access to certain content of the application may depend on the informed acceptance of a cookie or other such device, if it is used for a legitimate purpose. It is important 1 Article 29 working group guidelines - Available: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_maaruse_2016679_kohase_labipaistvuse_kohta.pdf 7 (8) obtain the voluntary, specific, informed and unequivocal consent of the user or opting out of cookies. If the user does not agree, the performance of the main functions of the application must still be guaranteed. The conditions for giving the data subject's consent are set out, among other things, in Article 7 of the General Regulation on the Protection of Personal

Data. We further explain that a compliant notification of the use of cookies includes an explanation for what purpose you use cookies, for how long and who are the various parties with whom you plan to share them (if any relevant). The notification should include a reference to the data protection conditions, where the conditions for the use of cookies are also explained. The data subject must understand which cookies the website collects and must be able to give separate consent or refusal for each type of cookie (except cookies that are essential for the website to function). As an example, you can take LHV Bank's cookie consent request form. Since Nerostein OÜ still does not ask data subjects for their consent to use cookies on its website, it is necessary to issue a prescription. Website security Although the Data Protection Inspectorate did not address the website security aspect in its previous explanations, this deficiency was also identified when the monitoring procedure was initiated. Namely, the website of www.nerostein.ee lacks a certificate, i.e. the connection is insecure. It can be seen on the website that it is also used to collect data, not just to display information. To the extent that data (including personal data) is collected on your website, the connection to the website must be made secure. (from HTTP to HTTPS) I add an explanation t explain their concepts - https://www.veebimajutus.ee/blogi/https-miks-see-sind-huvitama-peaks. Making changes takes less than 10 minutes. Article 32 paragraph 1 of the General Regulation on the Protection of Personal Data states that, taking into account the latest developments in science and technology and the costs of implementation, and taking into account the nature, scope, context and purposes of personal data processing, as well as threats of varying probability and size to the rights and freedoms of natural persons, responsible and authorized processors shall apply appropriate technical and organizational measures to ensure the corresponding security, including, among other things, as necessary, the provisions of paragraph 1 points a-d of the same article. At the present moment, it is clear that the HTTP connection on the website is not secure for the processing of personal data and it must be made secure, which is why a prescription is necessary in this case. /signed digitally/ Mehis Lõhmus lawyer on the authority of the director general 8 (8)