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. 2.2.-2/21/474 Injunction maker Data Protection Inspectorate lawyer Mehis Lõhmus Time and place of injunction 30.03.2021 in Tallinn Recipient of injunction - personal data processor Living Minerals OÜ address: Kivila tn 18, Tallinn 13917 e-mail address: living.minerals@gmail .com Person in charge of the personal data processor Member of the board RESOLUTION: § 56 (1), (2) point 8, § 58 (1) of the Personal Data Protection Act (IPS) and Article 58 (2) point d, Article 13 (1) point c of the General Regulation on Personal Data Protection (IKÜM), On the basis of d and f, I issue a mandatory order for compliance: 1. to bring the data protection conditions of Living Minerals OÜ into compliance with the requirements set forth in Articles 12-14 of the IKÜM. I set the deadline for the fulfillment of the injunction to be April 12, 2021. Report the fulfillment of the injunction to the e-mail address of the Data Protection Inspectorate at info@aki.ee no later than this deadline. 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. WARNING: If the injunction is not complied with by the set deadline, the Data Protection Inspectorate will impose a fine of 3,000 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(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: 1. On 03.02.2021, the Data Protection Inspectorate (AKI) received a notification from Living Minerals OÜ that a data leak had occurred. Namely, it was possible to access the personal data of customers on your website mineralgarden.org. 2. You wrote that the situation was brought under control in less than half an hour after CERT-EE was notified. You immediately deleted the available file, deactivated the plugins and also checked the website

settings to make sure that all possible threats have been eliminated. 3. The administrator of the website commented on the situation as follows: "It is a special feature of this module, which stored the export in the upload directory, which we were not aware of. The upload directory has always been public by default on wordpress, otherwise the images would not be displayed on the web. The data was certainly not found in the search engine, seo and webmaster block it by default, as well as wordpress itself. If someone found it in the upload directory and downloaded it, it is a deliberate attack against our page." 5. During the supervision procedure, AKI submitted an inquiry on 05.02.2021, to which Living Minerals OÜ responded on 10.02.2021. 6. Based on the answers received, AKI made an additional inquiry and made a proposal regarding the protection of personal data. 7. AKI proposed to draw up a privacy policy in accordance with Articles 12-14 of the General Regulation on the Protection of Personal Data, to immediately terminate the use of www.bluehost.com if there are no appropriate protection measures, and to issue the data of the webmaster. 8. On 22.02.2021, Living Minerals OÜ responded as follows: "We are preparing a new privacy policy and will announce its completion as soon as possible; Since the privacy policy of www.bluehost.com ensures the legal protection of European Union residents in accordance with the GDPR, we consider that there is currently no reason to terminate the contract with the service provider; The web administrator of www.mineralgarden.org is Online Sysadmin OÜ.“ 9. Since Living Minerals OÜ had not updated the data protection conditions long after the proposal was made, AKI made a repeated proposal on 17.03.2021 in the matter of personal data protection. 10. With the proposal, AKI wanted Living Minerals OÜ to draw up a privacy policy in accordance with Articles 12-14 of the General Regulation on Personal Data Protection and by March 25, 2021 at the latest. 11. On 26.03.2021, Living Minerals OÜ sent the following notice: "We drew up a new privacy policy in accordance with the guidelines of the Data Protection Inspectorate and uploaded upload it to the address https://mineralgarden.org/privaatsuspolitikami/." 12. AKI, having familiarized itself with the created data protection conditions, found that they do not meet the requirements set forth in Articles 12-14 of IKÜM. EXPLANATION OF THE PROCESSOR OF PERSONAL DATA: Response to the proposal made on 11.02.2021 Regarding the proposals: 1. We will prepare a new privacy policy and will announce its completion as soon as possible. Answer to the repeated proposal of 17.03.2021 We prepared a new privacy policy in accordance with the guidelines of the Data Protection Inspectorate and uploaded it to the address https://mineralgarden.org/privaatsuspoliitika/. GROUNDS OF THE DATA PROTECTION INSPECTION: The processing of personal data must be based on the principles of personal data processing (see article 5 of IKÜM). The processing of personal data must be legal, fair and transparent. The principle of transparency

requires that all information related to personal data processing (including data collection) is easily accessible, understandable and clearly formulated. To ensure transparency, it is necessary for the data controller to draw up and publish its data protection conditions. The content of the data protection conditions is regulated by Articles 12 - 14 of the IKÜM. You can also read more about transparency on pages 43 - 45 of the general manual for personal data processors prepared by the inspectorate (Chapter 10. Transparency1). We previously checked the data protection conditions of Living Minerals OÜ and found that they do not meet the requirements stated in articles 12-14 of the IKÜM. Below is an analysis of the data protection conditions of www.mineralgarden.org (Living Minerals OÜ): 1. In point 3 of the data protection conditions, you have stipulated the processing of customers' personal data. According to point 3.1, the data processor may process the following personal data of the data subject: first and last name; phone number; e-mail address; delivery address; current account number; payment card details; IP address. 2. In point 3.3, you have generally referred to Article 6 of the Personal Data Protection Act and said that "the legal basis for personal data processing is Article 6(1)(a,b,c and f) of the General Regulation on the Protection of Personal Data." 3. I explain that the basis for personal data processing cannot be entire article 6 of the IKÜM. In the interests of data subjects and general legal clarity, the legal basis must be clearly and comprehensibly referred to. For example: you list the different types of personal data that you process (first and last name, phone number, etc.) and you also write the legal basis behind each type. The data subject must have an understanding of the legal basis on which 1 General guide for personal data processors, Data Protection Inspectorate - Available: https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf (29.03.2021) this data is processed. 4. For the sake of clarity, I note that there are "articles" in IKÜM, not "sections". You must have mistakenly marked "section" in clause 3.3 of your data protection terms. 5. A personal recommendation (not an obligation) would be to make Chapter 3 in the data protection conditions in the form of a table, in the first column of which you list the data types, in the second column the legal basis and in the third column the purpose of the processing. 6. Imaginary example from the table: Data type Legal basis Purpose of processing First and last name IKÜM Article 6 paragraph 1 point b (agreement) Execution of the contract concluded with the client 7. I explain that the example given above is not a mandatory form. Nevertheless, this approach ensures an understanding of how and on what basis and what data is processed. 8. In clause 3.4 of the data protection conditions, you have outlined the purposes of processing personal data and the storage of personal data according to the purpose of processing. At this point, AKI recommends that retention periods be included as the fourth column in the table

shown above. Example: Data type Legal basis Purpose of processing Retention term First and last name IKÜM Article 6(1)(b) (agreement) Fulfillment of the contract with the client until the end of the contract 9. I explain that setting the purposes of processing is of little use if it is not clear which data will be processed more precisely. If in point 3.4.1 of the data protection conditions you have stipulated that the purpose of processing is security and safety, the question arises, which data is the purpose of processing security and safety? It is not unequivocally clear, and therefore it would be reasonable to use the table system referred to above or to explain in another way/supplement the points with the corresponding types of personal data. 10. The data protection conditions are completely missing the information resulting from IKÜM Article 13(1)(d), which stipulates that in case of data collection from the data subject, the responsible processor informs the data subject of information about the legitimate interests of the responsible processor or a third party. The data protection conditions do not specify the relevant legitimate interest of third parties in the processing of personal data, although it is specified as one of the legal grounds for processing in clause 3.3. 11. There is also no information from the data protection conditions about information transferred to third countries. For example, in your case, the leaked files were on a web server hosted by Bluehost, a service provider in the United States. According to Article 13(1)(f) of the GDPR, the data processor must disclose information that the data controller intends to transfer personal data to a third country or international organization, as well as information about the presence or absence of a commission decision on the adequacy of protection, or Article 46, 47 or 49, paragraph 1, second paragraph of the GDPR in the case of said transmission, a reference to the relevant or appropriate safeguards and the manner in which a copy thereof may be obtained or the place where they have been made available. In the current case, data subjects do not have information about the transfer of data to the United States, so it is extremely important that this requirement under the GDPR is met. About the background of the creation of the data protection conditions 12. I consider it necessary to explain that the data protection conditions are not simply "I do it, then I am in compliance with the law" conditions. Creating data protection conditions starts with an understanding of where, how and where data is moving. In most cases, such things can be detected by a data protection audit, for which sufficient material can be found on the Internet2. 13. An audit is probably not necessary for your company, because data processing is smaller compared to some IT companies. Nevertheless, you need to know how, on what legal basis and why the data is processed. This understanding must also reach the data subject, and that is what the data protection conditions are for. As mentioned before, the processing of personal data must be legal, fair and transparent, and the data protection conditions also help to fulfill these goals. Taking into account the factual circumstances and the fact

that the data processing is still ongoing, but the data subjects do not have adequate information about the data processing, AKI considers that issuing a mandatory injunction in this case is necessary to eliminate the violation. /signed digitally/ Mehis Lõhmus, a lawyer authorized by the general director 2 Examples of audits and their preparation - Available: https://www.aki.ee/et/inspektsioon-kontaktid/auditid (29.03.2021)