Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 PRELIMINARY WARNING in personal data protection case no. 2.2.-2/21/3026 Issuer of the injunction Data Protection Inspectorate lawyer Mehis Lõhmus Time and place of issuing the injunction January 5, 2022 Tallinn Recipient of the injunction - address of the personal data processor: e-mail address: jetskalo@severi.ee Responsible official of the personal data processor Sergei Jetskalo, management member (Severi Kaubandus OÜ) RESOLUTION: § 56 subsection 1, subsection 2 point 8, § 58 subsection 1 of the Personal Data Protection Act and article 58 subsection 1 point a of the General Regulation on Personal Data Protection and considering the same subsection with point e, the Data Protection Inspection makes Severi Kaubandus OÜ to comply with a mandatory injunction: Respond to the inquiry and proposal sent by the Data Protection Inspectorate on 09.12.2021 No. 2.2.-2/21/3026. 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: 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. 2 (4) 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. FACTUAL CIRCUMSTANCES: The Data Protection Inspectorate has a violation notification of Severi Kaubandus OÜ, according to which a cyber attack took place against Severi Kaubandus OÜ. Specifically, CERT-EE has found that "... Phobos ransomware was installed." Since installing ransomware requires gaining access to the device, the admed on the device should be considered leaked. Cybercriminals may later threaten to publish the collected data and demand a ransom. If the devices contained sensitive personal data, the Data Protection Inspectorate should also be considered." Therefore, we started a monitoring procedure based on § 56 (3) point 8 of the Personal Data Protection Act. The Data Protection Inspectorate has the right to request explanations and other information, including the submission of documents necessary for conducting the supervisory procedure.1 We asked you to fill in and submit the appropriate breach notification form and answer the questions posed in the inquiry. On October 14, 2021, you submitted the completed infringement

notification form and answered the questions. Insofar as the Data Protection Inspectorate identified deficiencies or inconsistencies in the answer you provided, we conducted a new inquiry on December 9, 2021 and also made a proposal. We identified the following problem areas in the inquiry of December 9, 2021: You have written in your answer that you do not know the exact number of persons affected by the attack. However, in the infringement notice, you stated that the number of persons affected by the infringement was 1-9. I explain that the number of persons affected by the breach means the exact number of persons whose data was leaked. Among other things, you have noted that 88.4 GB of data was leaked, so the number of personal data leaked may be large. In addition, you stated in the breach notification that the data subjects were informed verbally about the data breach and the following information was provided: "We had a cyber attack incident last night". The possibility of notifying data subjects remains unclear, because you have stated that the number of persons affected by the breach is unknown to you. Furthermore, we draw your attention to the fact that the above notification is incomplete. Pursuant to Article 34(1) of the General Regulation on the Protection of Personal Data, the data controller shall notify the data subject of a personal data breach without undue delay if the personal data breach is likely to pose a major threat to the rights and freedoms of natural persons. Paragraph 2 of the same article stipulates that in the notice provided to the data subject 1 Legal basis for asking for explanations: in the case of non-administrative persons, in accordance with § 30 paragraphs 1 and 3 of the Law on Law Enforcement together with Article 58 paragraph 1 points a, e and f of the General Regulation on Personal Data Protection; in the case of an administrative body, in accordance with § 752 (1) point 1. 3 (4) of the Government of the Republic Act, the nature of the violation related to personal data is described in clear and simple language and at least the information and measures referred to in points b, c and d of Article 33 (3) are presented. In this case, you haven't. In addition, you have not explained the reasons behind the data leak, incl. cause of leakage. I explain that the purpose of the breach notification is to provide the supervisory authority with the most accurate and clear overview of the data leak that has occurred, so that appropriate measures can be taken. We understood that Phobos malware was installed - but how did it succeed and what was missing from Severi Kaubandus OÜ's security side? Among other things, we asked the following questions in the additional inquiry: 1. What caused the leak? How did the attacker get access to the data? 2. Where was the data stored? 3. What security measures were implemented for data storage? 4. How much personal data was leaked? Please provide the exact number. If the number of leaked personal data is not yet clear, please give a reason and explain how it is planned to clarify this fact. 5. Why is the router replaced to prevent violations? How does changing your router help prevent future cyber

attacks? Why was such a decision made? 6. Has CERT-EE performed an in-depth analysis of the leak with recommendations and forwarded it to you? If so, please forward it to the Data Protection Inspectorate. In addition to the above, the Data Protection Inspectorate made a proposal to Severi Kaubandus OÜ: 7. to make a written notification to data subjects in accordance with the General Regulation on Personal Data Protection. In terms of the content of the notification, refer to Article 34, paragraphs 1 and 2 of the General Regulation on Personal Data Protection; 8. send a copy of the notification to the Data Protection Inspectorate. Unfortunately, to date, Severi Kaubandus OÜ has not responded to the Data Protection Inspectorate. We expected a response to the inquiry and proposal by December 17 at the latest. In the inquiry, the inspectorate also drew attention to the setting of an injunction and a fine in the event that the inspectorate's inquiry and proposal are not answered on time. GROUNDS OF THE DATA PROTECTION INSPECTION: In accordance with § 58 (1) of the Personal Data Protection Act and Article 58 (1) point a of the General Regulation on Personal Data Protection and taking into account point (e) of the same paragraph, the inspectorate has the right to request explanations and other information, including the submission of documents necessary for conducting the supervision procedure. Taking into account the factual circumstances and the fact that responding to the inquiry made as part of the supervisory procedure of the administrative body is mandatory, but Severi Kaubandus OÜ has not responded to the inquiry and proposal sent by the inspectorate on December 9, 2021, the inspectorate considers that issuing a mandatory injunction in this case is necessary supervisory matter 4 (4) to find out important circumstances and to carry out the administrative procedure effectively, including as quickly as possible. If the person has problems responding to the inspection by the specified deadline, the person can explain to the supervisory authority which objective circumstances were the obstacle. However, simply not responding is not acceptable. /signed digitally/ Mehis Lõhmus, a lawyer under the authority of the director general