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.-1/22/481 Issuer of the injunction Data Protection Inspectorate lawyer Geili Keppi Time and place of issuing the injunction 18.07.2022 in Tallinn Addressee of the injunction - personal data processor OÜ Krediidiregister e-mail address: art@krediidiregister.ee responsible person of the personal data processor Board member RESOLUTION Protection of personal data § 56 subsection 1, subsection 2 point 8 of the Act, § 58 subsection 1 and article 58 subsection 1 point a of the General Regulation on Personal Data Protection and taking into account the same subsection e in the specification of the inquiry sent on 04.07.2022 to the address info@aki.ee no later than 15.08.2022. 1. Please provide a comprehensive overview of the information system (www.taust.ee), which logs are generated from which operations in the systems. Including whether there are separate logs for views and downloads. 2. In addition to logging, describe other selected security measures with which the data processor fulfills the obligations of Articles 5 and 32 of the General Regulation? 3. Provide an overview of all log types with their retention times. 4. To clarify how long the logs created for X have been stored and to issue all existing logs. 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. PENALTIES WARNING: If the injunction has not been fulfilled by the specified deadline, the Data Protection Inspectorate will impose a penalty of 2,000 euros on the addressee of the injunction on the basis of § 60 (2) of the Personal Data Protection Act: a penalty of 2,000 euros for each point in the injunction not fulfilled. 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: On 11.02.2022, X submitted a complaint to the inspectorate, according to which Krediidiregister OÜ does not provide the complainant with the requested copy of the processing of his personal data. The inspectorate submitted the first proposal to the data processor in the matter of personal data protection on 04/07/2022 and started a supervisory procedure against OÜ Krediidiregister on the basis of § 56 (3) point 8 of the Personal Data Protection Act and asked Krediidiregister OÜ to respond to the complainant (sending a copy to info@aki.ee) the identity of the person by 21/04/2022 at the latest to the claim submitted on the basis of Article 15 of the

General Regulation on the Protection of Personal Data. On 12.04.2022, Krediidiregister OÜ responded to the inspection's proposal, but continued to not provide logs on the processing of the applicant's personal data. On 04.07.2022, the inspectorate submitted a clarification of the inquiry, where we explained that when using information systems containing all kinds of personal data, keeping logs is one of the main security measures of the data processor, because otherwise the data processor has no way of guaranteeing the principles of transparency and legality of data processing (unauthorized processing, quick detection of cyber attacks, etc.). As a result, the inspection asked to answer clarifying questions by 18.07.2022 at the latest. On 08.07.2022, Krediidiregister OÜ responded to the specification of the inspection's inquiry, but has still partially failed to actually answer the questions. PERSONAL DATA PROCESSOR'S EXPLANATION The data processor's answers to the clarification of the inquiry submitted by the inspection: Below are OÜ Krediidiregister's answers to the questions: 1. OÜ Krediidiregister does not manage the www.e-krediidiinfo.ee environment, therefore the company cannot describe the logs created in this system. In Taust.ee, viewings of personal cards, server-to-server requests and user logins through the Minu taust functionality are recorded. 2. A Legitimate Interest assessment has been carried out, i.e. the processing of various data has been assessed, procedures have been created to ensure the relevance, correctness and security of the data, their retention periods have been established. The data subject's inquiries will be answered within a maximum of 30 days. 3. Deadlines for logs related to payment disruptions: Personal data related to partners, service consumption and disputes are stored during the validity of the contract and for an additional ten years for the protection of possible legal claims. Payment defaults and related data are stored for a maximum of fifteen years, data on viewing payment defaults are stored for 5 years. 4. X payment default views are registered in the information system as follows: Krediidiregister OÜ added an extract from the history of payment default views. OÜ Krediidiregister would like to point out the factual circumstances related to X's enquiries: a) X sent OÜ Krediidiregister a statement on 27.11.2021 requesting the issuance of logs defined by X himself. X wanted information: 1) data on the alleged debt 2) the claimant (if it has changed by chance in the case of an item, state when) 3) who added the data 4) who changed the data b) OÜ Krediidiregister responded to the application sent on 29.11.2021 (2 days after receiving the application), information about the debt (answers to points 1 and 2 of the application) and an explanation that the data are being changed (initial data entry, later changes, e.g. adding a receipt) were sent by employees of Julianus Inkasso OÜ (answer to points 3 and 4 of the application). In the clarification of the sent inquiry, AKI writes: In this case, several entries have been made about X in the information systems (e.g. data entry entry), but after several requests, no logs concerning his

data have been provided to X. In the previous sentence, AKI writes: We explain that a person cannot demand that the logs be presented in the way he likes, but the data processor provides him with the logs in the form that he has. OÜ Krediidiregister: X has not asked OÜ Krediidiregister for a data entry (unfortunately, it remains unclear what is meant by this at all). The information about the payment default has been forwarded to the person, in addition, the sent response contained information about the claimant of the payment default. Due to the above, OÜ Krediidiregister does not agree with the statement of the Data Protection Inspectorate that OÜ Krediidiregister has not provided the logs after several requests. In addition, we specify that information about making inquiries and payment failures can also be seen in the My Background environment, which the user can use after identifying himself. GROUNDS OF DATA PROTECTION INSPECTION Pursuant to § 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. In the specification of the inquiry submitted by the inspectorate on 04.07.2022, the inspectorate wanted to receive answers to the following questions: 1. Please provide a comprehensive overview of both information systems (www.taust.ee and www.e-krediidiinfo.ee) separately, which logs are generated from which operations in the systems. Including whether there are separate logs for views and downloads. 2. In addition to logging, describe other selected security measures with which the data processor fulfills the obligations of Articles 5 and 32 of the General Regulation? 3. Provide an overview of all log types with their retention times. 4. To clarify how long the logs created for X have been stored and to issue all existing logs. In the following, we present Krediidiregister OÜ's answers (numbered according to the order of questions) and analyze their content: 1. OÜ Krediidiregister does not manage the www.e-krediidiinfo.ee environment, so the company cannot describe the logs created in this system. In Taust.ee, viewings of personal cards, server-to-server requests and user logins through the Minu taust functionality are recorded. According to Krediidiregister OÜ, viewings of personal cards, server-to-server requests and users' own logins are recorded in the taust.ee environment. It is not explained in detail what logs are generated from these actions and whether different logs are generated for views and downloads. It is also unclear whether the system creates separate logs about the entry of payment errors and whether the data processor has such logs. With this, we find that the question has not been answered and a comprehensive overview of all generated logs has not been provided. 2. A Legitimate Interest assessment has been carried out, i.e. the processing of various data has been assessed, procedures have been created to ensure the relevance, correctness and

security of the data, their retention periods have been established. The data subject's inquiries will be answered within a maximum of 30 days. The inspection explains that the basis for keeping a log results from the interaction of Articles 5 and 32 of the General Regulation. When processing personal data, the availability, integrity and confidentiality of the data must be ensured. Availability ensures the timely and easy availability of data to an authorized person or technical tool. Integrity means ensuring the correctness, completeness and relevance of the data and ensuring that the data comes from an authentic source and has not been altered without authorization. Confidentiality means the availability of data only to an authorized person or technical means. The assessment of legitimate interest and the provision of retention periods alone do not guarantee the availability, integrity and confidentiality of the data. The credit register does indicate that procedures have been created to ensure the relevance, correctness and security of the data, but fails to explain in what way and what procedures have been created for this purpose. It is not possible to understand from the answer how, for example, it is ensured that the data cannot be changed by unauthorized persons, or how, more precisely, the availability of data is ensured only to authorized persons and how it is checked. The data processor has a duty of proof, which he can only fulfill if the system creates corresponding logs of the data processing operations. Krediidiregister OÜ has not yet proven that they keep a log of who enters or changes the data, only an extract of the complainant's payment failure views has been submitted. If there are no such logs, the inspectorate cannot agree that procedures have been established to ensure the relevance, correctness and security of the data. If the data processor maintains information systems where no logs are created or he has changed the settings of the information system in such a way that they are not created or deleted automatically, such data processing is not allowed at all, as it clearly contradicts the main principles of the General Regulation. The answer refers to the assessment of legitimate interest, but no assessment of legitimate interest is attached. At the same time, the question has not been answered, nor has a description of other security measures been provided. 3. Deadlines for logs related to payment disruptions: Personal data related to partners, service consumption and disputes are stored during the validity of the contract and for an additional ten years for the protection of possible legal claims. Payment defaults and related data are stored for a maximum of fifteen years, data on viewing payment defaults are stored for 5 years. In this response, Krediidiregister OÜ confirmed that there are logs related to payment failures and that the logs have been kept for a long time. However, the inspection wanted to receive a specific overview of all log types, and this has not been provided. 4. Viewings of X payment failures are registered in the information system as follows (excerpt attached). The inspectorate asked to clarify how long the logs created for X are kept and to issue all existing logs.

Krediidiregister OÜ forwarded the extract only regarding the review of the applicant's payment irregularities. At the same time, he did not provide information on how long such logs are kept, nor did he make it clear that he has not created any other logs about the person. Consequently, we assume that some logs have been left unsubmitted. In the previous point (see answer 3), Krediidiregister OÜ confirmed that personal data related to partners, service consumption and disputes are stored during the validity of the contract and for an additional ten years for the protection of possible legal claims. Payment defaults and related data are stored for a maximum of 15 years, data on viewing payment defaults are stored for 5 years. In addition, Krediidiregister OÜ has confirmed that viewings of personal cards, server-to-server requests and users' own logins are recorded. However, an extract is presented only from X's payment default views. In the clarification of the inquiry made on 04.07.2022, the inspectorate explained that all logs that are linked to a specific person are considered personal data and the person can request the logs created about him. We explained that the person cannot demand that the logs be presented in the way he likes, but the data processor provides him with the logs in the form that he has. In response to the inspection, Krediidiregister OÜ finds that the applicant has not requested a data entry entry. In the first request made to Krediidiregister OÜ, the applicant wanted to receive a log file, among other things, about who added the data. Krediidiregister OÜ also referred to this same request in its response to the specification of the inquiry. As said, the person cannot demand it in any way he likes, and Krediidiregister OÜ really does not need to know exactly which natural person entered the data, but some kind of log should be created in order to fulfill the obligations arising from the general regulation, and a copy of it should be issued exactly as it is available to the data processor. is. In response to the clarification of the inquiry made by the inspectorate on 04.07.2022, OÜ Krediidiregister considers that it has forwarded the logs to the complainant, insofar as the information on when the payment default occurred was provided to the person in the response to the applicant's request, and in addition, the sent response contained information about the payment default claimant. We explain that the logs are related to the system, and based on the logs, it is possible to identify what has happened in the system and who has performed certain activities in the system. To the extent that all logs that are linked to a specific person are considered personal data and the person can request the logs generated about him, it cannot be accepted that in this case a copy of the requested log would have been forwarded to the person. Krediidiregister OÜ forwarded to the inspectorate only an excerpt of the inspection of payment irregularities. If Krediidiregister OÜ only has a log of payment default views, then in this case it is a violation, because if other logs are not kept, it is not possible to follow the principles of personal data processing and ensure the security of data processing. The use

of any information system generates automatic system logs, which is why it is vitally implausible to claim that the data processor does not have them. Taking into account the factual circumstances and the fact that responding to an inquiry made within the supervision procedure of an administrative body is mandatory and the inspection has the right to demand explanations and other information, including the submission of documents necessary for conducting the supervision procedure, but Krediidiregister OÜ has not answered the inspection's inquiry in substance, has not submitted all the logs and has partially ignored questions raised, the inspectorate finds that issuing a mandatory injunction in this case is necessary to find out the important circumstances of the supervisory case and to carry out the administrative procedure effectively, including as quickly as possible. /signed digitally/ Geili Kepp's lawyer under the authority of the General Director