PRIVACY PROTECTION AND STATE TRANSPARENCY Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 FOR USE WITHIN THE ORGANIZATION Information holder: Data Protection Inspectorate Note made: 01.02.2023 Access restriction valid until: 01.02.2 098; in terms of paragraph 2 until the decision made in the procedure enters into force Basis: AvTS § 35 paragraph 1 paragraph 2, AvTS § 35 paragraph 1 paragraph 12 PRELIMINARY WARNING in personal data protection case no. 2.1.-1/22/28852 Issuer of the injunction Data Protection Inspectorate lawyer Alissa Hmelnitskaja Time and place of issuing the injunction 01.02.2023 in Tallinn Recipient of the injunction - personal data processor XXX address: XXX e-mail address: XXX RESOLUTION: Paragraph 56 of the Personal Data Protection Act (IKS) 1, subsection 2 point 8, § 56 subsection 3 points 3 and 4, § 58 subsection 1, § 10 and on the basis of Article 58 subsection 1 point d and subsection 2 points f and g of the General Regulation on the Protection of Personal Data (IKÜM), also considering Article 6 of the General Regulation on Personal Data Protection , the inspectorate issues a mandatory injunction to comply with: 1. XXX to stop disclosing other people's personal data on personal and company "XXX" Facebook accounts. I set 15.02.2023 as the deadline for fulfilling the injunction. 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 Code of Administrative Procedure 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 set deadline, the Data Protection Inspectorate will impose an extortion fee of 1,000 euros on the recipient 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 FACTS: The Data Protection Authority (AKI) has received complaints regarding the fact that XXX

(controller/data processor) discloses other people's personal data both on his personal Facebook account and on his company's (XXX) account. Certain posts are related, among other things, to the disclosure of debt data of private individuals. Posts that contain personal data of other persons: On the controller's personal Facebook account: 1. The post made on 17.12.2022 at 16:59 contains the full names of persons XX and XX and a photo of person XX. On the Facebook account of the controller company: 1. The post containing personal data about XX was made on 11.12.2022 at 11:44; 2. The post containing personal data about XX was made on 06.12.2022 at 14:09; 3. The post containing personal data about XX was made on 30.10.2022 at 17:30; 4. Jt AKI started the supervision procedure on the basis of IKS § 56 (3) point 8, within the framework of which proposal No. 2.1.-1/22/2885 was made on 15.12.2022 for better compliance with the requirements for personal data protection. According to the proposal, XXX had to stop disclosing personal data of other persons on his personal and his company's "XXX" Facebook accounts and send a confirmation of this to the inspectorate no later than 29.12.2022. Due to the fact that the controller has asked to extend the deadline of 29.12.2022 for the proposal, the new deadline for completing the proposal was set for 06.01.2023. In addition, it was stated in the proposal that if the data controller does not agree with the proposal, he had to explain on what legal basis and purpose and reasons he publishes other persons' personal data on social media. On 13.01.2023, the data controller sent a response to AKI's proposal. In its response, the controller has explained the disclosure of personal data of only some people - XX, XX, XX, XX. Therefore, the data controller has only partially justified the disclosure of other people's personal data, but the Facebook group "XXX" page has published personal data about other people as well. For example: 1. A post made on 04.10.2022 at 15:33, which contains the personal data of people XX, XX and XX. On the computer network: X 2. A post made on 21.10.2021 at 20:08, which contains XX's personal data. On the computer network: X 3. A post made on 29.09.2020 at 17:57, which contains XX's personal data. On the computer network: X 4. 02.07.2020 at 17:09 a post made, which contains XX's personal data. On the computer network: X 5. 02.07.2020 at 17:08 a post made, which contains XX's personal data. In a computer network: X The controller's reasoning is as follows: 1. XX is the controller's YY, with whom the controller has communicated to find out what is going on in his/her YY's life. XX XX has called the controller to find out why the controller is communicating with XX. The data controller considers that it was an intimidation call, as XX spoke aggressively, and this type of speech caused non-pecuniary damage to the data controller. In this regard, the data controller stated the following as the reason for publishing the data of these persons: "Therefore, we also announced that the opportunity to repair the damage. We decided to publish the story, because such publication gives a clear signal to Other

Persons that Intimidation of Others, especially in a family where there is already chaos and minor children in the family, who should not see or experience the things that parents do wrong, will become established and will most likely become the norm. and is unacceptable in any case. We consider that such publication is in the public interest, which outweighs the interests of the given subjects, because the given information is true, it gives a signal that such activities are prohibited, which can always end in claims for damages in Court. I believe and I am convinced that when put on the scale, my interests outweigh the interests of the given person, because given the influence and YY trying to brainstorm, it is difficult to find solutions, all the more so that on 11.01.2023 there will be a call by a sworn lawyer by the Children's Protection Union, where we will discuss the issue of possible custody rights related to children and also asked if we are ready to be YY's guardian if necessary. Therefore, I find that if it really is me, if YY has no other options, where a pastor has also been used and other solutions have been tried, then not acting and watching and not intervening is completely contrary to the family law and understandably abnormal without the law. " 2. Regarding XX, the responsible processor explained that his YY took a loan from XX, and in connection with the fact that the debt had not been paid, XX began to write defamatory and insulting expressions. "This kind of activity, like everything I have pointed out in relation to XX, is unacceptable in this regard, and to label and identify as a criminal, if there is no basis for this, is to damage a strong legal interest and it definitely outweighs the rights of the given person not to be public, especially since it is with the truth. Here, too, we take the position that such a legal benefit would hardly be for the public, which truth would outweigh the suffering caused to YY. " 3. XX is the controller YY. The controller claims that YY has failed to pay tenants and also owes money to relatives and friends. The controller intends to go to court with the aim of restricting or incapacitating YY because YY has a drug, alcohol and casino addiction. Thus, the controller collects information about YY, namely about possible (financial) claims against him. "We decided to publish the story because such publication sends a clear signal to Others that such behavior is unacceptable. " 4. Regarding XX, the responsible processor explained that the data of this person had been forwarded to Creditinfo AS. "So a person threatening to call the police and asking us to exercise our rights is blatantly indifferent and we treat it as blackmail on His part. …. . So we also announced that the opportunity to repair the damage. We decided to publish the story because such publication sends a clear signal to Others that such behavior is unacceptable. Taking the above into account and as of 01.02.2023, the data controller has not fulfilled proposal No. 2.1.-1/22/2885, as he continues to disclose other people's personal data on his personal Facebook account and on his company's Facebook "XXX" account. GROUNDS FOR THE DATA PROTECTION INSPECTION: 1. Legality of personal data

processing According to article 4 point 1 of the GDPR, personal data is any information about an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be directly or indirectly identified, in particular on the basis of an identification feature such as name, social security code, location information, network identifier or on the basis of one or more physical, physiological, genetic, mental, economic, cultural or social characteristics of that natural person. Therefore, personal data includes, among other things, a name, a photo of the person and other information that enables the identification of the person. The requirements for personal data processing are primarily established by the IKÜM, Article 5 of which stipulates the principles of personal data processing, including the principle of legality. The processing of personal data (including disclosure on the Internet) is legal only if there is a legal basis for this in Article 6, paragraph 1. The data controller has stated in his answer that "Is there a difference if one speaks to another, another to another, etc., etc., where everyone knows later or the majority or publicly. There is no logic, because if today I were to send an individual message to everyone on Facebook, for example 2,500 friends, then they, in turn, etc., etc., this is allowed, but not like that. However, if I collect 5000 friends in all environments and put etc. etc. to everyone, then it can be like that, but isn't it already public when word of a certain circle spreads? Of course it is. It is no longer in a certain circle, but has gone out of the circle, where there is even less control, to whom and how far it spreads, but it spreads and it is already in the open". The inspectorate does not agree with the controller's position that if he forwards data to third parties (the controller's Facebook friends, of which there are, for example, 2,500), then it would not be a violation. Therefore, the inspection considers it necessary to clarify the following. Recital 18 of the IKÜM states that this regulation should not be applied to the processing of personal data carried out by a natural person exclusively for personal or domestic purposes and therefore outside of professional business activities. Personal and home activities could include correspondence and mailing lists or activities on social networks and the Internet that are conducted as part of such personal or home activities. Therefore, considering that the controller constantly discloses the personal data of various people, and most of the posts are made on his company's Facebook page, which has 613 followers, it appears that the data is not disclosed between close relatives, the scope and frequency of this data processing indicate a commercial purpose, and this data processing entails negative consequences for the data subjects. consequences. Taking into account the above, the data processing in dispute does not fall under the exception of Article 2(2)(c) of the IKÜM. In connection with this, the requirements arising from the IKÜM must be applied in this situation. The principles of personal data processing are set out in Article 5 of the General Data Protection Regulation, which must be followed by the controller,

including the principle of legality. The processing of personal data is legal if it corresponds to one of the legal bases set out in Article 6 of the IKÜM (consent, performance of a contract, legal obligation, protection of vital interests, for the performance of a task in the public interest or for the exercise of public authority, legitimate interest). 1.1. In order to process personal data on the basis of Article 6(1)(f) of IKÜM, i.e., legitimate interest, the data processor must be convinced that the purpose of personal data processing is more important than the rights and freedoms of the data subject and Articles 21 (right to object) and 17 (right to deletion of data) of IKÜM ) the processing of personal data must be stopped if the data processor cannot prove that the processing is for a compelling legitimate reason that outweighs the interests, rights and freedoms of the data subject. In the current case, it does not appear that the data processor can rely on the legal basis of legitimate interest, since he has not submitted a legitimate interest analysis to the inspection. The data controller has explained that by publishing personal data, it sends a signal to other people that certain behavior is not allowed and that publishing is in the public interest, which outweighs the interests of the data subjects, because the information given is true, but mere statements are not enough to process personal data. The processing of personal data on the basis of a legitimate interest must be preceded by an analysis by the data processor regarding the legitimate interest and importance of the data processor and third parties, an analysis of the rights and interests of the data subject and their importance, and then a weighing between the interests of the data processor and the data subject. 1.2. IKS § 4 In certain cases, the disclosure of some people's data may be justified for journalistic purposes. According to § 4 of the IKS, personal data may be processed without the consent of the data subject for journalistic purposes, in particular disclosed in the media, if this is of public interest and is in accordance with the principles of journalistic ethics. The disclosure of personal data must not excessively harm the rights of the data subject. In order to disclose personal data based on § 4 of the IKS, three conditions must be met: 1. there is a public interest in the disclosure of personal data; 2. the disclosure is in accordance with the rules of journalistic ethics; 3. the disclosure of personal data must not excessively harm the rights of the data subject. According to AKI, the criterion of public interest is not met in this case. The existence of public interest can be confirmed if the topic raised and personal data disclosed contribute to the debate in a democratic society. However, disputes arising in human relationships are in no way related to the public interest, and disclosing the personal information of a single individual does not contribute to the social debate. The same rationale applies to the disclosure of debtors' data. If an opinion piece were published about why loans are taken lightly in Facebook groups in Estonia and, on the contrary, loans are given, but the fact of the indebtedness of each individual natural person does not fall into the

sphere of public interest, the publication of which would contribute to the further development of a democratic society. 1.3. § 10 of IKS § 10 of IKS can be used to disclose debtors' data, which stipulates that the disclosure of personal data related to a breach of debt relationship to a third party and the processing of transmitted data by a third party is permitted for the purpose of assessing the creditworthiness of the data subject or for other similar purposes, and only if all three conditions: 1. the data processor has verified that there is a legal basis for data transmission; 2. the data processor has checked the correctness of the data; 3. the data transfer is recorded (keeping information about who and what was transferred). Information on who has an overdue debt against whom, how much it is (including ancillary claims), when it occurred and what type of transaction is considered to be payment default data. In the current case, it does not appear that the posts containing the debtors' personal data are disclosing the indebtedness of a specific person with the aim of protecting other persons from making bad deals. Even if it is assumed that the purpose of the posts corresponds to § 10 of the IKS, the assumption that the controller would have checked the legal basis for the transfer of personal data remains unfulfilled. However, the data controller has made the debt data publicly visible to the unlimited public, which means that it cannot control who sees the data, and thus cannot control whether the recipient of the data has a legal basis. Debt relationships between people, including rights and obligations arising from loan agreements, are regulated by the Law of Obligations Act (VÕS), which provides legal remedies in case of breach of contract - VÕS § 101. However, none of the legal remedies prescribed by law provide for the right to disclose the debtor's personal data. Taking into account the above, the inspection is of the opinion that in this case none of the legal bases specified in Article 6, paragraph 1 of IKÜ exist for the disclosure of other people's personal data, and the data processor has not proved to the inspection that the legal basis for disclosing debtors' data derives from § 10 of the IKS. Personal data has been processed without legal baseless, which is why the controller must stop disclosing posts containing other people's personal data on social media. In accordance with IKS § 58 (1) and IKÜ Article 58 (2) f and g, the inspectorate has the right to issue an order to limit the processing of personal data. Taking into account that in a particular case, the personal data of natural persons is disclosed illegally and that the data controller did not agree to the Data Protection Inspectorate 19.04 .2021 to comply with the proposal, the inspectorate considers that issuing a mandatory injunction in this case is necessary in order to end the offense as soon as possible. (digitally signed) Alissa Khmelnitskaja lawyer under the authority of the Director General