

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.-1/23/2891-5

Issuer of the injunction Data Protection Inspectorate lawyer Alissa Hmelnitskaja Time and place of issuing the injunction
10.03.2023 in Tallinn Addressee of the injunction - personal data processor XXX e-mail address: XXX RESOLUTION: § 56
subsection 1 of the Personal Data Protection Act (IKS) , paragraph 2 point 8, § 58 paragraph 1, § 10 and on the basis of Article
58 paragraph 1 point d and paragraph 2 points f and g of the General Personal Data Protection Regulation (GPR), as well as
taking into account Article 6 of the General Personal Data Protection Regulation (GPR), the Data Protection Inspectorate
issues a mandatory prescription for compliance: 1. Stop disclosing other people's personal data in the Facebook group "XXX"
managed by XXX, without the consent of Article 6(1)(a) of IKÜM. I set 24.03.2023 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 1,500 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 CIRCUMSTANCES: The Data Protection Inspectorate (AKI) is
in the process of a person's complaint regarding the disclosure of debt data of private individuals in the Facebook group "XXX".
Therefore, AKI initiated the supervision procedure. As part of the supervisory procedure, on 26.01.2023, AKI made a proposal
to XXX (hereinafter also the data processor or responsible processor) in personal data protection case no. 2.1.-1/23/2891-2,

the content of which was as follows: "stop the disclosure of posts containing personal data in the Facebook group managed by you "XXX". The deadline for responding to the proposal was 10.02.2023. In the proposal, AKI drew attention, among other things, to the possibility of making an injunction and imposing a penalty payment, and the right to submit one's opinion and objections to the matter in accordance with § 40 (1) of the Administrative Procedure Act before issuing an administrative act. The data processor has received AKI's proposal and on 09.02.2023 expressed a desire to talk with the official. The conversation took place on 15.02.2023 by phone, during which the official gave additional explanations about the proposal. As of 10.03.2023, the data processor has not fulfilled AKI's proposal. GROUNDS FOR THE DATA PROTECTION INSPECTION: According to article 4 point 1 of the IKÜM, 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, primarily based on such identification as name, personal identification number, location information; but also based on one or more physical, physiological characteristics of this natural person. Thus, personal data also includes a person's name, image and other information that enables the identification of a person. In this case, it is a public Facebook group in which posts containing other people's personal data are made. Certain posts are warnings, i.e. the purpose of the post is to warn other people to avoid entering into transactions with persons whose personal data is disclosed. At the same time, these posts are also made in this group, the purpose of which is to influence the debtor and pressure the debtor to pay off the debt. Examples: 1) The post was made on 19.02.2023 at 13:02. On the computer network: XXX 2) The post was made on 19.02.2023 at 13:00. On the computer network: XXX 3) The post was made on 19.02.2023 at 13:06. On the computer network: XXX 4) The post was made on 19.02.2023 at 13:01. On the computer network: XXX 5) The post was made on 19.02.2023 at 13:06. In a computer network: XXX 6) Cont. According to article 4 point 2 of the IKÜM, the processing of personal data is an automated or non-automated operation or a set of operations performed with personal data or their collections, including their distribution or disclosure by making them available in another way. Article 4 point 7 of IKÜM states that the responsible processor is a natural or legal person, public sector institution, office or other body, which alone or together with others determines the purposes and means of personal data processing. Facebook has determined that the group administrator (or data processor) has full control access to the Facebook group. This means that the data processor can change the name of the group or its privacy settings, can delete posts and comments written about it.¹ It follows that, as the administrator of the disputed Facebook group, the data processor has the opportunity to change the name of the given group and delete posts made in the group and comments

made about it. In addition, the data processor, as an administrator, has assigned the name of this group to "XXX" and has made this group public, with which he has clearly directed the discussion in the group (created the group with the aim that users can make posts on specific topics) and thanks to the fact that the data processor made the group public, personal data will be disclosed there unlimited for everyone. Taking into account the above, AKI considers that the data processor is the responsible processor according to Article 4, Clause 7 of IKÜM, as it determines the purposes of personal data processing (group name, rules) and means (choice of social media platform, public group). The data processor, as the administrator of the group, is responsible for ensuring that the disclosure of data is legal². 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. IKÜM article 6 paragraph 1 point a IKÜM article 6 paragraph 1 point a 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. IKÜ Article 4, point 11, consent is defined as "a voluntary, specific, informed and unequivocal expression of will by which the data subject, either in the form of a statement or by an action expressing clear consent, agrees to the processing of personal data about him": a) The word "voluntary" means a truly free choice for the data subject and check. In general, the GDPR stipulates that if the data subject does not have a real choice, if he feels compelled to consent, or if he has to endure negative consequences if he does not give consent, the consent is invalid. If consent is part of non-negotiable terms, it will not be considered voluntarily given. Thus, consent is not considered voluntarily given if the data subject cannot refuse or withdraw consent without adverse consequences. b) "Specific" means that the data subject's consent must be given "for one or more specific purposes". According to IKÜM Article 5(1)(b), obtaining a valid consent is always preceded by the determination of the precise, clear and legitimate purpose of the intended processing. The need for specific consent together with the purpose delineation in accordance with Article 5(1)(b) prevent the gradual expansion or blurring of the purposes of data processing after the data subject has given his consent to data collection. c) IKÜM strengthens the requirement that consent must be informed. On the basis of Article 5 of IKÜM, one of the basic principles is transparency, which is closely related to the principle of legality and justice. Providing information to data subjects before obtaining their consent is important to enable data subjects to make an informed decision, to understand what they are agreeing to and, for

example, to exercise their right to withdraw consent. 1 Facebook Help Center:

<https://www.facebook.com/help/901690736606156>; https://www.facebook.com/help/289207354498410?helpref=faq_content 2

Similarly, the European Court has reached the conclusion in decision C-210/16 that the administrator of the Facebook page is a data controller within the meaning of Article 2 point d of Directive 95/46. d) It is clearly stated in IKÜM that consent requires a statement from the data subject or a clear action expressing consent, which means that it must always be given by taking active steps or submitting a confirmation. It must be obvious that the data subject has consented to the specific processing. The silence or inactivity of the data subject and the mere continuation of using the service cannot be considered as making an active choice. In addition, the controller must bear in mind that the responsibility of proving consent rests with him. As a result of the above, the data controller cannot rely on Article 6(1)(a) of the IKÜM, as it has not provided AKI with proof that the disclosure of personal data takes place with the consent of the data subject and that the consent is valid in accordance with the requirements set forth in Article 4, Clause 11 of the IKÜM. 2. In order to process personal data on the basis of article 6 paragraph 1 point f of Article 6 paragraph 1 point f of IKÜM, or 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 on the basis of data deletion) 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. The processing of personal data on the basis of a legitimate interest must be preceded by an analysis carried out by the data processor in terms of 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.³ AKI is of the opinion that the processing of personal data for the sole purpose of public warning is not legitimate on the basis of a legitimate interest. In addition, the controller has not submitted a legitimate interest analysis to AKI. 3. IKS § 10 In addition to the legal bases given in Article 6 of the IKÜM mentioned above, it is possible to rely on IKS § 10 for the disclosure of debtors' data, which stipulates that the disclosure of personal data related to the violation of a debt relationship to a third party and the processing of the transmitted data by a third party is permitted for the purpose of assessing the creditworthiness of the data subject or for another similar purpose, and only if all three conditions are met: 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 transmission is registered (keeping information about who and what was transmitted). In

this case, according to AKI, the assumption that the data controller would have checked the legal basis for transferring personal data has not been met. However, the controller has made the debt data publicly visible to the unlimited public, which means that the controller cannot control who sees the data and therefore cannot control whether the recipient of the data has a legal basis. In addition, according to IKS § 10 (2) point 3, the processing of a person's debt data (including on Facebook) is not permitted if it would excessively harm the rights and freedoms of the data subject. Therefore, the data processor has to assess, based on the circumstances of each specific case, whether the right to data processing outweighs the interference caused to the privacy of the person or not. AKI is of the opinion that in this case the disclosure of personal data of various people is large-scale, as it is carried out via the Internet (including Facebook). Disclosure of data on the Internet increases people's vulnerability, as this environment is sometimes uncontrollable and it is not possible to identify who has received information related to personal data and what they do with this information. Therefore, on the basis of IKS § 10, the prerequisites for disclosure of personal data are not met. 4.

3 AKI Legitimate Interest Guide, page 6. Available online: https://www.aki.ee/sites/default/files/dokumendid/oigustudu_huvi_juhend_aki_26.05.2020.pdf

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. The latter could be the case, for example, if an opinion piece was published, for example, about why loans are taken lightly in Facebook groups in Estonia and, on the contrary, loans are given, but the publication of personal data of individual debtors does not have the power to advance such a discussion. Also, the data processor has not proven to AKI that the requirements of the code of journalistic ethics have been met, as the data subject is not heard before publishing the debt data (p. 4.2 of the code) and he is not given the opportunity to object (p. 5 of the code). AKI is of the opinion that data processing is accompanied by an obvious invasion of privacy of data subjects, which, in addition to the lack of a legal basis, is also excessive considering the composition of the

data. For example, it is not permissible to disclose photos of the debtor or other people, complete extracts of conversations held with the person(s), etc. Since the criteria for the application of IKS § 4 have not been met, personal data cannot be disclosed on the basis of IKS § 4. AKI notes that in the case of payment defaults, it must be borne in mind that in the event of indebtedness, the creditor must primarily use the legal remedies listed in § 101 of the Law of Obligations Act, one of which is the demand for performance of the obligation, in order to achieve payment of the debt. It is not permissible to publish personal data on payment defaults only as a pressure measure to achieve debt payment. Taking into account the above, AKI is of the opinion that in this case, none of the legal bases specified in Article 6, paragraph 1 of IKÜM exist for the disclosure of other people's personal data, and the data processor has not proved to AKI that the legal basis for data disclosure derives from § 10 of IKS. Personal data has been processed without without a legal basis, which is why the controller must stop disclosing posts containing other people's personal data in the Facebook group "XXX". According to IKS § 58 paragraph 1 and IKÜM art 58 paragraph 2 points f and g, the inspectorate has the right to issue an order to limit the processing of personal data. Taking into account that in this particular case the personal data of natural persons is disclosed illegally and that the data controller has not complied with AKI's proposal of 26.01.2023, AKI considers that issuing a mandatory injunction in this case is necessary in order to stop the infringement as soon as possible. (digitally signed) Alissa Khmelnietskaja lawyer under the authority of the Director General