

www.aki.ee Registration code 70004235 PRESCRIPTION-WARNING in personal data protection case no. 2.1.-6/22/1

Prescription author Raiko, lawyer of the Data Protection Inspectorate Kaur Time and place of making the injunction

19.01.2022, Tallinn Recipient of the injunction responsible person Krediidiregister OÜ (12400621) art@krediidiregister.ee

art@taust.ee Board member RESOLUTION: § 56 subsection 1, subsection 2 clause 8 of the Personal Data Protection Act

(IKS), Section 58(1) and Article 58(1)(d) and Paragraph 2(d) and (f) of the General Regulation on Personal Data Protection

(IKÜM), as well as taking into account Articles 5, 6, 7, 12 and 14 of the General Data Protection Regulation, the Data

Protection Inspektsioon Krediidiregister OÜ issues a mandatory injunction to comply with: Terminate on the website

www.taust.ee data processing (collection, disclosure) of natural persons (including representatives of legal persons) until: 1.

The file of all valid and invalid documents related to the legal person has been completed open-ended disclosure of private

data of private persons (payment defaults, tax debts, number of real estates, official announcements and court decisions) (see

subsection 3.1 of the grounds of the Data Protection Inspectorate); 2. When issuing data, the existence of a legitimate interest

of each third party is checked (assessed) or categories are determined (e.g. tenant, borrower, employee/business partner) on

which it is possible for a third party to carry out a background check (see Subsection 3.2 of the reasons of the Data Protection

Inspectorate); 3. When issuing data, the scope of the data is limited in accordance with the interests of the third party (the

recipient of the data) (see sub-point 3.2 of the grounds of the Data Protection Inspectorate); 4. Issuance of data to unidentified

persons (users not logged in) has been stopped (see subsection 3.2 of the reasons of the Data Protection Inspectorate); 5.

The disclosure of invalid connections on the personal card of a natural person with whom the data subject has not had contact

or for whom there is no such need has been completed (see subsection 3.3 of the reasons of the Data Protection

Inspectorate); 6. Before disclosure of personal data, documents proving indebtedness are checked (see Tatari tn 39 / 10134

Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 Data Protection Inspectorate's reasons subsection 3.5);

7. The inspection has been provided with a clear and comprehensible legitimate interest analysis that meets the conditions set

out in Article 6(1)(f) of the IKÜM, i.e. by reading it, it is possible for both the inspection and the data subject to clearly

understand the following (see subsection 3.6 of the Data Protection Inspectorate's reasons): a) what are Specific legitimate

interests of Krediidiregister OÜ and third parties; b) for what reason is the scope and method of personal data processing

actually necessary for the realization of the legitimate interests specified in point a; c) what are the rights and freedoms of the

data subject that are violated during the processing of personal data; d) how do the legitimate interests of Krediidiregister OÜ and third parties (points a and b) outweigh the interests and fundamental rights of the data subject (point c); 8. The data protection conditions have been brought into line with the requirements set forth in Articles 12 and 14 of the IKÜM (see subsections 3.4 and 3.7 of the reasons of the Data Protection Inspectorate); 9. The use of third-party cookies on the website is terminated until the person's consent to the use of cookies in accordance with Article 7 of the IKÜM is obtained (see Subsection 3.7 of the reasons of the Data Protection Inspectorate); 10. The inspectorate is assured that upon receiving the contact details of the data subject, the data protection conditions will be forwarded to the data subject in accordance with article 14, paragraph 3 of the GDPR (see subsection 3.7 of the grounds of the Data Protection Inspectorate). We set 18.02.2022 as the deadline for fulfilling the injunction. If at least one of the points of the injunction is not fulfilled by the specified deadline, the processing (collection, disclosure) of personal data of natural persons (including representatives of legal entities) on the website [www.taust.ee](http://www.taust.ee) must be stopped by the specified deadline. Report compliance with the order to the e-mail address of the Data Protection Inspectorate at [info@aki.ee](mailto: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.

**EXERCISE MONEY WARNING:** If the injunction has not been complied with by the specified deadline, the Data Protection Inspectorate will impose a fine of 10,000 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 (1) of the Personal Data Protection General Regulation may result in a misdemeanor proceeding based on § 70 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. Tatari tn 39 / 10134 Tallinn / 627 4135 / [info@aki.ee](mailto:info@aki.ee) / [www.aki.ee](http://www.aki.ee)

Registration code 70004235 **FACTUAL CIRCUMSTANCES:** On 25.07.2017, the Data Protection Inspectorate (inspection)

started self-initiated monitoring (monitoring) on the basis of § 33 (5) of the Personal Data Protection Act in force at the time. , the purpose of which was to map the situation of personal data processing in information portals. The aim of the conducted monitoring was to find out which personal data and on which legal basis information portals are collected and (re)disclosed, and how people are informed about aspects related to privacy. At the beginning of 2018, the inspectorate sent Krediidiregister OÜ an interim monitoring summary regarding the (re)disclosure of personal data in information portals, and we also drew attention to the fact that from the application of the General Regulation on the Protection of Personal Data (GPR), if necessary, the inspectorate will take measures to ensure the legal situation in accordance with the conditions stipulated in GPR. Based on this, we notified on 21.05.2019 of the supervision procedure initiated on the basis of § 56 (3) point 8 of the Personal Data Protection Act (IPS), the purpose of which was to check compliance with the requirements set forth in the Personal Data Protection Act. In connection with the ongoing supervision procedure, we conducted an additional analysis in the light of IKÜM and forwarded to Krediidiregister OÜ on 01.06.2020 the position and proposals of the Data Protection Inspectorate for better compliance with the Personal Data Protection Act (hereafter we refer to the document as the 01.06.2020 proposal). In the 01.06.2020 proposal, we pointed out, among other things, the following: 3. Data protection conditions must be drawn up and disclosed on the website, which fully meet the requirements set forth in Articles 12 - 14 of the IKÜM. 4. A document must be drawn up that would describe the existence of a legitimate interest in sufficient detail (analysis/assessment). 5. The obligation is to ensure that the data subject has the opportunity to submit an objection, including the obligation to resolve the objection based on the content of the objection. In a situation where the data subject's request is not satisfied, the information portal must prove that there is a valid legitimate reason for further processing. 6. Additional protective measures must be implemented - for example, to ensure greater transparency for data subjects and to create an electronic environment that allows to see, use and object to personal data. The Data Protection Inspectorate has the right to request explanations and other information, including the submission of documents necessary for conducting the supervisory procedure,<sup>1</sup> therefore respond to the following no later than July 10, 2020: 1. Specify a specific date when you will bring your activities into line with the above proposals (positions). 2. If you do not agree with the proposals of the inspection, please highlight a specific point or position of the proposal and your own objections in this regard. In the 10.07.2020 response, Krediidiregister stated that the data protection conditions have been disclosed on the website and the legitimate interest analysis has been carried out. On 18.12.2020, a representative of Krediidiregister OÜ submitted an analysis of the legitimate interest and explained the

implementation of additional protective measures: a) OÜ Krediidiregister has performed an analysis of the legitimate interest of itself and its customers. b) The person who made the request is identified, a fee is charged for the request and the existence of a legal basis is checked. c) Notifying data subjects if the data exists d) The data subject has the opportunity to view various data related to him/her, regarding them

1 Legal basis for asking for explanations: in the case of non-administrative persons, according to § 30 paragraphs 1 and 3 of the Law on Law Enforcement Act together with Article 58 paragraph 1 points a and e of the General Regulation on the Protection of Personal Data; in the case of an administrative body, in accordance with § 752 subsection 1 point 1 of the Government of the Republic Act.

Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee

Registration code 70004235 to provide feedback (submit objections), an information system with corresponding functionality has also been created for this purpose the types of all official announcements that are published on the website were communicated and it was explained that there are no court decisions in the taust.ee environment, the taust.ee environment performs a query and directs the court decision to the Riigiteataja environment to view. On 29.11.2021, the inspectorate issued an injunction to gain access to the taust.ee website, and on 01.12.2021 Krediidiregister OÜ complied with the injunction. We further explain that although the inspection referred to the repeated inquiry sent on 18.11.2021 in the said order, we were wrong about the year and the actual date was 18.11.2020.

REASONS FOR THE DATA PROTECTION INSPECTION: 1.

Processing of personal data Personal data is any information about an identified or identifiable natural person. An identifiable natural person is a person who can be directly or indirectly identified, primarily based on his or her identification, such as name, personal identification number, etc. (see article 4, point 1 of IKÜM). Therefore, the data of all natural persons related to legal entities (e.g. name, personal identification number, connection with the legal entity) are personal data and within the scope of application of IKÜM. Data that do not fall within the scope of IKÜM are data that concern only legal entities, i.e., for example, the name of a legal entity and the contact details of a legal entity (see Recital 14 of the IKÜM). Also, the (re)disclosure and combination of the data of legal entities, for example, with the debts of a legal entity is not within the scope of IKÜM. Based on this, the position of the inspectorate does not deal with the processing of data of legal entities, but only the processing of data of natural persons (including people related to legal entities). The object of the supervisory procedure is the processing of personal data, which concerns the collection of data of natural persons (including representatives of legal persons) from various sources and their subsequent disclosure on the website www.taust.ee (hereinafter taust.ee). The Data Protection Inspectorate checked the compliance of the website taust.ee with the principles of personal data processing (Article

5 paragraph 1 of IKÜM) as part of the supervision procedure. Krediidiregister OÜ was responsible for proving compliance with IKÜM requirements (Article 5 paragraph 2 of IKÜM), which is why we can evaluate and analyze the documents that have been submitted to the inspection as part of the supervision procedure and make a decision based on the documents submitted to the inspection and found on the website. We also checked the actual data processing on the taust.ee website.

### 1.1. Processing of personal data on the taust.ee website

The Inspectorate logged in to the taust.ee website to see the view of the logged-in user. The user can make inquiries based on the company name and registry code as well as the name and personal identification number of a natural person.

#### 1. During the inspection of the website, we found that when making a query by company name/registry code, the following personal data is displayed (hereinafter company card):

- 1.1. Name and personal identification number of related persons (e.g. board member);
- 1.2. Name and personal identification number of invalid related persons (e.g. former board member) and period of board membership;
- 1.3. The number of payment defaults, tax debts, properties and official announcements and court decisions of both related parties and invalid related parties (e.g. 1 payment default, 2 properties).

#### 2. It is then possible to open each natural person (both former and current board members)

Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 separately. It is also possible to do this as a separate search based on a specific natural person (name, personal identification number). The personal card of a natural person (hereinafter referred to as the personal card) displays:

- 2.1. business network;
- 2.2. related (natural) persons;
- 2.3. related companies;
- 2.4. invalid related (natural) persons;
- 2.5. invalid related companies;
- 2.6. number of payment defaults, tax debts, properties, official announcements/judgments.

#### 2.6.1. If there are payment defaults, tax debts, real estate, official announcements/judgments, a pop-up window will appear before viewing them:

I hereby confirm that I will use the received data in accordance with the purpose (to assess creditworthiness) and have a legitimate interest in viewing the payment defaults of the following persons: [Front – and surname (identity code )]

Misuse of the received data entails liability under debt law as well as misdemeanor liability both to the sender of payment default data and to the person with payment defaults. By pressing "ok", the information is displayed as follows:

- payment errors are displayed on the taust.ee portal. Content: claimant, date of claim, end date, field (e.g. other financial services), indebtedness (reported amount of total indebtedness), status (e.g. disclosed);
- tax debts are displayed on the taust.ee portal. Contents: date, tax debt, including postponed, including disputed;
- in the case of real estate, the e-real estate book is redirected and a new inquiry must be made there to familiarize with the real estate;
- to familiarize yourself with court decisions, on the riigiteataja.ee page, you are directed to a specific court decision that

applies to a person; - official announcements are displayed on the taust.ee portal. In addition, on the taust.ee website it is possible to: 1) download in pdf form or immediately print out the identity card displayed on taust.ee. It is possible to tick 1) personal data, 2) related companies, 3) related persons. When you put a check mark in front of the personal data, a pop-up window appears (see content above), on which the personal data opens when you press "ok"; 2) add private individuals to monitoring (monitoring of tax debts, monitoring of payment defaults, monitoring of official announcements); 3) the user can check when and for whom a specific request has been made. For example, if the company has several users, it is possible to view individual requests for each user (user, date and who was viewed); 4) search for claims (debts) of natural persons and import them into the computer; 5) add a requirement of a natural person. Mandatory fields – name, social security number, e-mail address or phone number, amount of debt, currency, percentage of late payment per day, date of claim and on how many days the debt will be published ("publish after x days"). Optional fields - city, address, index, e-mail or phone, fine, payment schedule, comment (it is possible to write a comment in the box). 6) by logging into taust.ee, the natural person can check who (name of the legal entity) and on what date has checked payment defaults. It is also possible for a non-logged-in user to buy an identity card - you have to enter the identity code and check the box "I confirm that I have a legitimate interest in viewing the payment defaults of the person (identity code...)". It is also possible for a non-logged-in user to enter a private person's claim (disclose debtors). For this purpose, the creditor's data (name, telephone and e-mail) and the debtor's data (name, personal identification number, debt amount) must be transmitted. It is possible to voluntarily transmit additional information (additional information box) and add basic documents. Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 Based on the above, personal data is processed on the taust.ee website, which must be based on the requirements set forth in the IKÜM. During the inspection, we also evaluated the actual data composition, that is, we randomly evaluated the content of official announcements and court decisions published on the website. We also assessed the manner in which personal data is disclosed. Krediidiregister OÜ has explained that personal data is processed on the basis of legitimate interest. In addition, taust.ee users are asked to confirm that the received data is used to assess creditworthiness and that a third party has a legitimate interest in obtaining the data.

## 2. Principles of personal data processing

The processor of personal data is obliged to comply with the principles set forth in Article 5, paragraph 1 of the IKÜM. The responsible processor himself is responsible for the fulfillment of these principles and must be able to prove their fulfillment (see IKÜM Article 5 paragraph 2). To the extent that data processing does not fully comply with the principles set forth in

Article 5, paragraph 1 of the IKÜM, data processing is prohibited. In the proposal of 01.06.2020, we outlined the mandatory principles of personal data processing and explanations regarding them: - Lawfulness, fairness and transparency (IKÜM Article 5 paragraph 1 point a) Any processing of personal data must be fair and legal, i.e. fully in accordance with all applicable legislation (including IKÜM and with IKS). Data processing must also be transparent. The principle of transparency requires that all information related to the processing of personal data is easily accessible, understandable and clearly formulated for the data subject. This primarily concerns the notification of data subjects in order to ensure fair and transparent processing (see Recital 39 of the IKÜM). Informing people is more precisely regulated by articles 12 - 14 of the IKÜM. Articles 13 and 14 of the IKÜM state what the information given to a person must contain as a minimum. To a large extent, however, information portals must be based on the requirements of Article 14 of IKÜM, since data is not usually collected from the person himself. At the same time, we emphasize that each data processor himself must ensure that his data protection conditions meet the requirements of IKÜM. Within the framework of this supervision procedure, the inspectorate has reviewed the data protection conditions of all information portals, and it must be noted that deficiencies, including significant deficiencies, have been identified in several data protection conditions. Therefore, all information portals must be reviewed and made sure that their data protection conditions meet the requirements stated in the articles of IKÜM. We recommend point by point to review all the requirements set forth in Articles 13 - 14 of the IKÜM and assess whether and in which point of the data protection conditions these requirements are regulated. Regarding the data protection conditions, it is possible to read more precisely in the general manual of the personal data processor prepared by the inspectorate (Chapter 10. Transparency; Appendix 3. Data protection conditions control questionnaire). In addition, several information portals noted that people are not informed separately about the processing of their data, but it is possible to obtain this information from the data protection conditions published on the website. However, the inspection was not given a reason on the basis of which information is not issued to people. Given that data (for example, business register data, court decisions) is not collected from the person himself, the information portal is obliged to provide the person with the information provided for in paragraphs 1 and 2 of Article 14 of the IKÜM within a reasonable time, but no later than one month after receiving the personal data or if the personal data is intended to be disclosed to another recipient, then at the latest at the time of the first publication of the data (see IKÜ Article 14 paragraph 3).

Tatari tn 39 / 10134 Tallinn / 627 4135 / [info@aki.ee](mailto:info@aki.ee) / [www.aki.ee](http://www.aki.ee) Registration code 70004235 The differences that allow to bypass the active notification of a person result from Article 14 paragraph 5 of the IKÜM, i.e. information does not have to be

forwarded if: a ) the data subject already has this information; b) providing this information proves impossible or would require a disproportionate effort; c) the receipt or disclosure of personal data is expressly provided for in Union or Member State law, which provides for appropriate measures to protect the legitimate interests of the data subject; d) personal data must remain secret due to the duty of professional secrecy regulated by Union or national law, including the statutory duty of secrecy. Point d does not apply to information portals. Point c requires that the receipt or transfer of data is expressly provided for in Union or Member State law. However, this is not provided for by EU or Estonian law for information portals. On the basis of point a, notification can be omitted if, for example, the bank informs a person that it will transfer his debt data to the non-payment register and also includes the data protection conditions of the specific non-payment register. Point b could be the basis for failure to notify, especially in a situation where the information portal does not have the contact details of a specific natural person (data is not collected). At the same time, according to the inspection, information portals should not collect additional personal data only in order to fulfill the obligation of active notification. If the information portal has the contact details of a natural person, the person must be informed about the data processing and it is not an impossible or disproportionate effort. According to Article 13(1)(e) and Article 14(1)(e) of the IKÜM, the data processor is also obliged to inform the person to whom his personal data may be transferred. In the data protection conditions, it is possible to categorize the receivers (e.g. lessors, lenders) in case there are no definite and specific receivers (legal entities). However, if a person specifically asks for the person to whom his personal data has already been transferred, the data processor is also obliged to identify the specific recipient (see IKÜM Article 15(1)(c). Therefore, already as a result of IKÜM, the data processor has the obligation, if necessary, to prove the person to whom the information about the person has been transmitted. In the case of data related to the violation of a debt relationship, the obligation to register data transfer is also confirmed by IKS § 10 paragraph 1. Thus, the information portal is obliged to register every single data transfer, and the person has the right to receive information about who, when and to whom his data was transferred. The information portal also has the obligation to prove, if necessary, the legal basis and purpose for which the data was issued to a third party. - Purpose and retention limitation. Collecting as little data as possible (Article 5(1)(b, c and e) Personal data may be processed only to the extent that is unavoidably necessary to achieve predefined goals. The scope also means the time scope - the processing must be stopped and the data deleted or transferred to a non-personalized form as soon as the legal basis ceases and/or the purposes for which they were collected have been fulfilled. The time for processing personal data must be strictly limited to the minimum. In order to ensure that



personal data are not processed longer than necessary, the data controller must determine the deadlines for deleting personal data and for periodic review (see also justification point 39 of the IKÜM). - Correctness of data (IKÜM Article 5(1)(d)) When processing personal data, it must be ensured that the personal data is correct and, if necessary, updated, and that all reasonable measures are taken so that incorrect personal data from the point of view of the purpose of the processing is deleted or corrected without delay. Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 Therefore, the information portal has an obligation to ensure the correctness of all processed personal data (e.g. violation of previous contractual obligations, amount of debts). This is especially important in situations where data is transferred and/or made public. Processing false data can cause significant harm to a person. Checking the correctness of data and its importance is also emphasized in IKS § 10. - Reliability and confidentiality of data (IKÜM Article 5(1)(f)) When processing personal data, it must be ensured that personal data is processed in a way that ensures appropriate security of personal data, including protection against unauthorized or illegal processing for and against accidental loss, destruction or damage using appropriate technical or organizational measures. The information portal must ensure that only those persons who have the right to do so (i.e. there is a legal basis for obtaining the data) can access the collected personal data. This is also confirmed by IKS § 10, according to which the controller must check the existence of a legal basis. Therefore, the information portal itself must assess whether personal data can be transferred (access granted) to a specific person requesting the data and, if necessary, create technical and/or organizational measures to check this. The data processor must also review whether the level of security is still sufficient, either after a certain period or in the light of specific cases (see also Article 32 of the IKÜM). In a situation where the level of security does not exclude the dangers arising from illegal processing (including data transfer), the level of security must also be increased, that is, both technical and organizational measures must be made more efficient. If the data processor relies on a legitimate interest in the processing of personal data, it is legal if the processing of personal data is necessary for the legitimate interest of the data controller or a third party, unless such interest is outweighed by the interests of the data subject or the fundamental rights and freedoms for which personal data must be protected (Article 6 paragraph 1 point f of IKYM). Thus, IKÜM article 6 paragraph 1 point f stipulates three conditions, all of which must be met in order for the processing of personal data to be permitted: - the controller or the third party or third parties receiving the data have a legitimate interest in data processing; - the processing of personal data is necessary for the exercise of a legitimate interest; - the legitimate interests of the data controller and/or third party outweigh the interests, fundamental

rights and freedoms of the protected data subject. In order to understand whether it is possible to process personal data on the basis of Article 6(1)(f) of the IKÜM, it is first necessary to find out exactly whether and what is the legitimate interest of the information portal itself and the legitimate interests of a specific third party and/or the public. The legitimate interests of both the information portal itself and third parties (including the general public) must be formulated clearly enough. This requires a real and present interest – something related to an activity currently taking place or a benefit expected to be received in the near future. In other words, interests that are too vague or speculative are not enough. If the legitimate interests are not formulated clearly enough, it is not possible to balance said interests with the interests and fundamental rights of the data subject. Therefore, it is first of all important that the legitimate interest is in accordance with the current legislation, formulated clearly enough (ie sufficiently specific) and real and present at the moment (ie not speculative). Secondly, it is necessary to analyze and consider what are the possible interests or fundamental rights of the data subject - and freedoms that may be harmed by the processing of personal data. Thirdly, the legitimate interests of the information portal and/or third parties must be balanced with the interests and fundamental rights of the data subject. In doing so, the possible impact on the data subject from the processing (collection, transfer, disclosure) of personal data is compared with the legitimate interests of the controller and/or third party, and it is assessed whether and to what extent the legitimate interest of the controller and/or third party outweighs the interests of the data subject. We emphasize that the legitimate interests of the controller or a third party do not automatically outweigh the interests related to the fundamental rights and freedoms of the protected data subjects. The above evaluation is done abstractly, without distinguishing each specific data subject. However, a new legitimate interest assessment must be carried out at the level of a specific data subject if the data subject submits an objection to the information portal on the basis of IKÜM to the processing of personal data concerning him, which is carried out on the basis of Article 6(1)(f) of IKÜM (see Article 21(1) of IKÜM). The mentioned provision obliges the data processor to respond to objections and, within this framework, to conduct an additional analysis based on the situation of a specific person, as a result of which it becomes clear whether the further processing of data regarding a specific person is justified or not. If the data processor fails to perform one of the previous steps correctly, the data processing is not permitted on the basis of Article 6(1)(f) of IKÜM. In the 01.06.2020 proposal, the Inspectorate thoroughly analyzed the legitimate interest used in information portals and will not repeat it in this document. In the following, we describe the data processing that takes place at taust.ee and assess its compliance with the principles of personal data processing.

### 3. Compliance with IKÜM requirements

#### 3.1. Disclosure of personal data for the purpose

of checking the legal entity's right of representation and reliability Both valid and invalid connections are displayed on the Taust.ee company card. For each natural person, the information about them, i.e. the number of payment defaults, tax debts, properties and court decisions/official announcements is listed. It is then possible to click on the name of each natural person and see the identity card of a specific person and open all the information about the private person upon confirming the existence of a legitimate interest. For the sake of simplicity, we refer to this as private data or private data. For example, on the taust.ee page, the inspectorate identified a situation where a company partner was deleted from the business register based on an application submitted in 2012. However, the said partner continues to be displayed on the Taust.ee website under invalid related persons of the aforementioned company and his private data is displayed. The private activity of a natural person and the activity of a legal entity must be kept separate and they may not be reported together as a general rule. In the context of assessing the trustworthiness of a legal entity, a legitimate interest in the personal payment and contractual behavior of a private individual may exist in exceptional cases. This can come into question if the reliability of the legal person depends on the creditworthiness of the natural person, i.e. especially if the natural person is responsible for the obligations of the legal person with all his assets (e.g. FIE, full partner of a limited partnership). If Krediidiregister OÜ considers that in some cases it is necessary to display the private data of related natural persons when checking the reliability of a legal entity, a correct legitimate interest analysis must be made in this regard, which would show that data processing in this way and to this extent is actually necessary and how this need outweighs the interests of the data subject - and fundamental rights.

Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235

### 3.2. Transfer of data to third parties (disclosure to the public)

On the taust.ee website, payment defaults, tax debts, the number of properties, official announcements and a reference to a specific court decision are disclosed. The inspection stands by the views stated in the proposal of 01.06.2020, therefore, in the opinion of the inspection, the transmission of the above information in the information portal is permitted if: a) only data concerning violations of contractual obligations are processed and; b) data transfer is based on the recipient of the data or each request is evaluated separately before the data is issued. With regard to data concerning violations of contractual obligations, we emphasize that the general public (i.e. an unlimited circle of persons) cannot disclose the data of a private person with the abstract purpose of "evaluation of a person". The public's abstract interest in evaluating a natural person does not qualify as a legitimate interest because it is not sufficiently clearly defined, concrete or actually existing (it is speculative). Although on the taust.ee page it is possible to get access to personal data for a fee and by confirming the

existence of a legitimate interest, it is still a service aimed at the general public, i.e. anyone can pay for the service and receive the data by clicking the "ok" button (confirming the legitimate interest). The inspection identified that natural persons are referred to court decisions that do not concern the assessment of creditworthiness - for example, we identified court decisions regarding drug handling and violations of traffic regulations. Referral to such court decisions is in any case excessively damaging to the data subject and does not in any way fulfill the purpose of creditworthiness assessment. Although the referral to the Riigiteataja page is inherently less offensive than the display of court decisions on taust.ee's own website (the content and retention period are regulated in the Riigiteataja), even in the case of a referral, personal data is processed (Krediidiregister OÜ has searched for court decisions concerning the person), which must be answered in the IKÜM to the stated requirements, i.e. data processing must be legal and purposeful. In addition, Krediidiregister OÜ has also stated in the confirmation requested from a third party: I hereby confirm that I use the data received in accordance with the purpose (to assess creditworthiness) and have a legitimate interest.... It remains unclear how a third party receiving the data can use drug handling or traffic violations to assess creditworthiness. Nor is it a breach of contractual obligations. Thus, Krediidiregister OÜ initially issues such data, in which the principle of purposefulness has been violated and in which a third party cannot have a legitimate interest in assessing creditworthiness. Regarding Official Announcements, Krediidiregister OÜ listed the types of announcements that are published on the taust.ee website. However, during the spot check, we identified, for example, one type of announcement that Krediidiregister OÜ did not list, i.e. "notice of declaration of invalidity of power of attorney". In the said notice, one private person declared invalid all the powers of attorney issued by him to another private person. Therefore, it remains unclear whether Krediidiregister OÜ has deliberately omitted to name all types of Official Notices that are disclosed on the taust.ee website, or whether Krediidiregister OÜ itself does not have an understanding of the actual data composition. In addition, it remains unclear why such an announcement is made public on the taust.ee website. Regarding the release of personal data to third parties, we admit that it is impossible to foresee all cases in which a third party may have a legitimate interest in checking the reliability of a private person, but despite this, Krediidiregister OÜ cannot offer an abstract private person assessment service, but must adapt it based on the recipient of the data. In other words, a solution must be created that takes into account which data someone (and if at all) has the right to receive in which case. Of course, it is possible that the information portal evaluates each request separately before issuing the data. Unfortunately, it would be so labor-intensive that it would probably make the service significantly slower, less efficient and more expensive. Tatari tn 39 / 10134 Tallinn /

627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 One option is to prepare standard services for the most common situations. In this way, some information portals have also classified the service according to the purpose – tenant background check, borrower background check, employment background check, business partner background check. In the general plan, the inspection also agrees with this classification. If the assessment of payment defaults and tax debts is necessary for each of the aforementioned background checks (provided that it is not excessively harmful to the data subject), the justification for transferring other data on the fulfillment of contractual obligations to date (which may be contained in court decisions, official announcements) depends on the person against whom the background check is performed. In the case of the tenant, for example, violations of the lease agreement (destruction of property) and official announcements of eviction notices may be relevant. As part of the background check of the employee/business partner, for example, violations of contractual obligations. It is understandable that it is not possible to list here in advance all the cases and situations that may be necessary to fulfill a specific goal. Each information portal must itself, based on the principles set forth in Article 5, paragraph 1 of the IKÜM, assess whether a specific breach of contractual obligation is related to and necessary within the context of a specific type of inquiry (e.g. background check of a tenant, borrower, employee, business partner). However, Krediidiregister OÜ has not developed standard services for different situations and does not check the existence of a separate legal basis for each application. The only action to view private data is confirmation through the pop-up window. However, according to the inspection, this is not sufficient - it is not possible to limit the composition of the data based on the recipient of the data. In addition to the above, it is also possible to buy a personal card for a user who is not logged in, for whom it is enough to enter the person's personal code and check the box to confirm legitimate interest. Transferring private person data in this way is prohibited - Krediidiregister OÜ cannot check the existence of a legitimate interest or prove to whom the data of a natural person was transferred. For example, it is also possible to buy personal data from a private person. To summarize the above, we repeat what was already stated in the proposal of 01.06.2020: In the case of background checks for private individuals, it is necessary to define on whom (e.g. tenant, borrower, employee/business partner) the background check is to be carried out and, based on this, to delimit the data composition. It is forbidden to transfer data to such an extent that it does not comply with the principle of purpose limitation and the processing of as little data as possible or excessively damages the data subject. If the background check categories are not defined, the presence of a third party's legitimate interest must be checked separately for each request, and the data composition must be defined accordingly.

### 3.3. Related (natural) persons

and invalid related (physical) persons displayed on the Taust.ee personal card The Data Protection Inspectorate did not understand the logic on the basis of which related persons and invalid related persons are associated with a specific data subject (the person about whom the inquiry is made). This logic is also not visible in the data protection conditions. It seemed to the inspectorate that those persons with whom legal entities are managed together are displayed under related natural persons (i.e. under related persons are members of the board). At the same time, it was not complete, perhaps we also identified a situation where a person who is on the board of the company jointly with the data subject was not displayed under related persons. Therefore, the inspectorate is not convinced that this logic is true. Under invalid related natural persons, we identified those persons who are current board members or members of the supervisory board of a former company related to the data subject. In other words, in the identified case, the data subject was last a shareholder of the company in 2012, and the current board members and council members of this company are displayed under invalid related persons of the data subject. However, here too we identified situations where it was unclear whether and for what reason a person was included under an invalid related person. For example, we identified the name of a person who has not been part of any legal entity related to the data subject. Therefore, the inspectorate is not convinced here either that the logic that the inspectorate came to is true. In any case, it is forbidden to display on the taust.ee personal card Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 such connections with which the person has not actually had contact (i.e. members of the management board or members of the council appointed after the person's association with the named company). In this case, it is wrong information, and the disclosure of information in this way can excessively harm the data subject. Namely, a situation may arise where, in the case of an invalid connection, it may be a person whose behavior (payment delays, tax debts) may put the data subject in an unfairly bad situation. If it is desired to continue data processing in this way, Krediidiregister OÜ must prepare a legitimate interest analysis, which would show why it is necessary to display related persons on the personal identity card of a natural person, including invalid related persons. You also need to understand its logic and set a retention period.

3.4. Score of a natural person Assigning a score (point total) to a natural person in the information portal may be allowed on the basis of legitimate interest for the purpose of assessing creditworthiness, taking into account the IKÜM profiling rules. Mh, each person must understand how and based on what his score has been formed (see also IKÜM point 60). However, it is certainly not allowed to compile, let alone disclose, any abstract human score that takes into account circumstances unrelated to creditworthiness (e.g. court decisions regarding drug handling or traffic violations). Although the inspection did not establish

during the random inspection that a score is assigned to a natural person, Krediidiregister OÜ has asked for clarifications on what information must be disclosed in such a case, and the data protection conditions also state that profiling is done on the basis of legitimate interest. We clarify that, regarding the performance of a profile analysis (scoring), information must be provided in the data protection conditions about the logic used and the importance and predictable consequences of such personal data processing for a natural person (see IKÜM Article 13(2)(f), Article 14(2)(g) and IKÜM recital 60).

### 3.5. Verification of the correctness of the claim (indebtedness) of a natural person

Pursuant to Article 5(1)(d) of the IKÜM, the publisher of the debt data must make sure that the published data is correct. If valid data taken from state registers can be assumed to be correct (e.g. tax debt to the Tax and Customs Board), then in the case of debt data received from private persons, the correctness of this data must be checked before passing it on to third parties. In this regard, the Supreme Court has specified that the keeper of the default register must check the notice of payment default sent by the creditor with sufficient thoroughness, if he had such an obligation and also the opportunity. In that case, it is not enough to only ask the original sender about the existence of the debt, but the controller must have more precise data that would confirm the existence of the debt<sup>2</sup>. When determining the existence of indebtedness, the bases given in § 82 of the Law of Obligations Act (VÕS) must be followed. It is important to keep in mind that the mere issuing of an invoice as a general rule does not prove the existence of a debt relationship or indebtedness, and vice versa - not receiving an invoice is not a justification for not paying for the service used. If the alleged indebtedness has arisen during the provision of a service, for example, a contract proving the provision of the service should be requested, if the indebtedness has arisen from a sales contract, then, for example, a deed of handover, warranty papers. The correspondence between the parties during pre-agreement negotiations can also be of decisive importance, from which it becomes clear when and what obligations the debtor is obliged to fulfill and whether he has violated them, i.e. a debt has arisen. However, if there are no documents proving the violation, it is not possible to prove <sup>2</sup> See more precisely the views of the Supreme Court's Civil Board decision No. 2-17-1026 of 13.03.2019 (paragraph 24).

Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235

correctness of the data and disclosure of the data is not allowed. This does not mean that the debt has not actually arisen or that the creditor cannot collect the debt through the court, but the disclosure of (debt) data without specific evidence is excessively damaging to the data subject, and such data processing does not meet ANY requirements. In addition, the situation where the debt is disclosed without concrete evidence and the non-incurrence of the debt must be challenged and proved by the data subject himself is not fair. On the

taust.ee website, it is possible to add a claim of a natural person for both logged-in users and non-logged-in users. In either case, there is no obligation to provide documents proving the occurrence of indebtedness, i.e. Krediidiregister OÜ does not check the correctness of the data. According to the inspection, the disclosure of data collected in this way is prohibited, i.e. the processing of personal data is not fair and the correctness of the data is not guaranteed.

### 3.6. Legality of personal data processing (legitimate interest)

Krediidiregister OÜ has forwarded to the inspection on 18.12.2020 a legitimate interest analysis, which the inspection checks for compliance with IKÜM requirements. We emphasize that the analysis of the legitimate interest must cover the entire part of the processing of personal data processed on the website, and in a situation where Krediidiregister OÜ is unable to prove the legal basis for the processing of personal data in any part or fails to do so, further processing of personal data is not allowed in this part either.

- Legitimate interests of Krediidiregister OÜ and third parties and their necessity

Krediidiregister OÜ has identified business interest, i.e. earning income, as its own legitimate interest. The content of the provided service is the collection, analysis and transmission of various information about both legal and natural persons. The company's cooperation partners (persons who purchase the service) are companies that make credit decisions/evaluate the reliability of potential cooperation partners, i.e. OÜ Krediidiregister customers have a legitimate interest in viewing the information necessary to make a credit decision. A credit decision is an economic decision in which someone gives someone their property in the hope of getting it back later on commercial terms. In other words, a person has a legitimate interest in getting to know certain data that helps to make sure that the credit decision is justified. With regard to the legitimate interest of third parties, it is stated: OÜ Krediidiregister clients have a legitimate interest in viewing the said data composition, i.e. natural persons have given OÜ Krediidiregister the right to the client to make a credit decision about themselves (applied for a loan or installment payment, expressed a desire to enter into a duration contract, which assumes financial obligations in the future - i.e. OÜ Krediidiregister customers are obliged to make sure that the person can fulfill the obligation). Or OÜ Krediidiregister's client is verifying the reliability of a legal entity in connection with the conclusion of a contract/transaction, which is why information is needed about both the specific legal entity and the individuals related to it. ' In practice, it is a widespread approach that the credit ratings of related parties are used in the evaluation of small or start-up companies, because there is no data on the company itself (e.g. the annual report has not yet been submitted) or the quality of this data is questionable. OÜ Krediidiregister collects and publishes verified information that is in accordance with applicable laws and court rulings (e.g. deadline for publishing defaults). The company has introduced various measures to verify data (e.g.



updating data from RIK) and created processes to exclude possible false data processing (notification of persons, data verification procedures based on received feedback, etc.). In addition, the company has defined the scope of data processing, i.e. that the minimum necessary data is processed, processing is terminated based on the fulfillment of the objectives or the termination of the legal basis. Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235

According to the inspection, Krediidiregister OÜ's legitimate interest in data processing can be derived from a business interest. There is also an understandable need to provide a service to companies that make credit decisions/assess the trustworthiness of potential cooperation partners. However, it remains unclear on the basis of which Krediidiregister OÜ claims that clients have a legitimate interest in viewing data, i.e. natural persons have given Krediidiregister OÜ the right to make credit decisions about themselves or the client is verifying the reliability of the legal entity in connection with the conclusion of the contract/transaction. Although Krediidiregister OÜ confirms that the client has a legitimate interest in checking the creditworthiness of the individual before transferring the data of the private person, this is not sufficient - i.e. it does not allow to state unambiguously and with certainty that the third party actually has a legitimate interest in obtaining personal data. In addition, it is possible to buy data from a user who is not logged in, that is, Krediidiregister OÜ cannot limit the fact that data cannot be bought by, for example, private individuals. The inspection also does not agree with the fact that Krediidiregister OÜ processes minimally necessary data. Krediidiregister OÜ indicates on the website that the data can only be used to assess creditworthiness, but the data collected and transmitted are not related to this - e.g. drug handling and violations of traffic regulations. In addition, the transmission of data is not based on the recipient of the data, i.e. all possible links to court decisions are transmitted to the third party, which refer to the person, regardless of whether the recipient of the data actually needs the data. In addition, it remains unclear: 1. Why is it necessary to display the private data of all related natural persons (including invalid related persons) on the company card. Although Krediidiregister OÜ has not clearly justified this need, indiscriminately displaying the private data of all related natural persons is prohibited and does not comply with the principles of limitation of purpose, collection and storage of as little data as possible. If Krediidiregister OÜ wants to continue to display the private data of a private person on the company card, then a correct legitimate interest analysis must be performed, which would show in which cases (in which part) the disclosure of private data is necessary when evaluating a legal entity; 2. Why is it necessary to display persons related to the person (including invalid persons) on the personal card. At the same time, those persons with whom the data subject has not actually had contact are displayed under invalid related (physical) persons. Also,

the logic on the basis of which the data subject is associated with third natural persons remains incomprehensible. 3. Does the taust.ee website include a point score for a natural person, if so, this legitimate interest must also be reflected in the analysis.

In addition, it remains unclear what Krediidiregister OÜ meant by profiling in the data protection conditions. - Interests or fundamental rights and freedoms of the data subject In this point, it is important to thoroughly analyze the possible interests or fundamental rights and freedoms of the data subject that may be harmed by the processing of personal data. Considering the capabilities of the website taust.ee, in the opinion of the inspectorate, Krediidiregister OÜ has significantly neglected the interests of the data subject. For example, the following are not considered: 1) Risk (threat), which concerns the possible submission of incorrect claims (debts) and therefore the possible illegal disclosure of data. This can be due to both the creditor's malice (presenting a claim that does not exist) and the fact that there is no clear evidence that the debt has arisen. The latter can be used by creditors, for example, because it is foreseen that due to the lack of evidence, it is not possible to collect the debt through the court. The likelihood of this risk is increased by the fact that claims can also be made by users who are not logged in. 2) The risk of possible illegal transfer of data. Firstly, Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 Krediidiregister OÜ does not verify the existence of a third party's legal basis (only confirmation is sufficient) and secondly, data is also transmitted to unidentified third parties (background on the website. e.e. persons not logged in). For example, a private person can also buy data. 3) Data is transferred to a third party to a greater extent than is actually necessary. Krediidiregister OÜ does not check the legitimate interest of a third party for each request, nor has it limited the composition of the data based on the recipient of the data. In addition, Krediidiregister OÜ directs you to read court decisions that are not related to the assessment of creditworthiness. 4) Private data of all related natural persons (including invalid related persons) is displayed on the company card. Data is also displayed for those natural persons whose data transmission is not and cannot be necessary to assess the reliability of the legal entity. 5) The personal card displays related persons (including invalid persons) with whom the data subject has had no contact or the connection has been minimal and a long time ago. There is also no transparency, based on which it would be possible to understand how the connections have been created and how long the connections are displayed. 6) If a point score is also added to a natural person, there is no information on what the point score is based on and what the consequences are for the data subject. It is understandable that the point score can affect, for example, obtaining a loan, and in a situation where the point score is based on unproven requirements, it can cause significant damage to the data subject. 7) It is possible to include natural persons in monitoring

(monitoring of payment debts, monitoring of payment defaults, monitoring of official announcements). Krediidiregister OÜ has not explained whether and for what reason it is necessary to include a private person in the monitoring and what it can bring to the person, including that it is not analyzed in the legitimate interest analysis. However, if it is a service during which the user of taust.ee is informed when the profile of the person added to the monitoring has changed (e.g. the added person has defaulted on payment), it is a very intensive hacking, i.e. continuous collection and monitoring of information. - Balancing the legitimate interests of Krediidiregister OÜ and the third party and the interests, fundamental rights and freedoms of data subjects. Since Krediidiregister OÜ has not analyzed the necessity of processing all personal data (the existence of a legitimate interest) clearly and comprehensibly, and not all important interests of the data subject that may be harmed by processing personal data have been identified. , it is not possible to correctly balance interests. However, we reviewed Krediidiregister OÜ's explanations and submit our comments. The fact that the data of a natural person can only be seen by paying customers, and the existence of a legitimate interest must be confirmed before seeing the data, is an additional restriction on viewing the data, but it does not guarantee that the transfer of data and the receipt of data are legal. According to the inspection, Krediidiregister OÜ must either check the presence of a legitimate interest in each request separately or limit the data composition according to the purpose of the data request (e.g. renting, business partner control, lending). Although there is also a risk of the latter being issued illegally, the composition of the transmitted data can be defined based on the recipient of the data, which is mandatory due to the IKÜM. Krediidiregister OÜ has stated: Various measures have been taken to ensure the correctness of the data, such as informing individuals, the possibility of filing complaints, procedural rules for dealing with complaints, etc. According to the inspection, the aforementioned activities are not related to ensuring the correctness of the data. In order to ensure the correctness of the data, Krediidiregister OÜ must check whether the submitted claims (debts) have actually been proven, i.e. there are documents confirming the debt. In this case, however, Krediidiregister OÜ does not do this. However, as regards notifying persons Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 and the possibility of submitting an objection, these are obligations arising from the IKÜM (see articles 12 – 14 and 21 of the IKÜM ), not by implementing additional protective measures. In terms of additional protection measures, it is stated that the data subject has the opportunity to view the data related to him, to give feedback on them (to submit objections), and for this purpose an information system with the corresponding functionality has been created. In the opinion of the Inspectorate, this is important and necessary in order to ensure the easiest possible way for the data subject to

get acquainted with his data and to submit objections. However, this alone is not enough. In a specific case, the scope and method of personal data processing on the taust.ee website excessively violates the data subject's rights, and the fact that the data subject can object to possible illegal data processing is not sufficient. It is not fair if every data subject has to deal with Krediidiregister OÜ's violations (e.g. disclosure of an illegal or unproven claim) due to non-compliance with ALL requirements. Based on the above, the legitimate interest analysis prepared by Krediidiregister OÜ is not sufficient, which is why the processing of personal data is illegal. In the event that a natural person's debts are illegally disclosed, it is a very serious offense (this can prevent both getting a job, getting a rental apartment, and getting a loan). Therefore, it is particularly important that a correct analysis of the legality of personal data has been carried out before processing personal data. The analysis of the legitimate interest must clearly understand: a) what are the specific legitimate interests of Krediidiregister OÜ and third parties; b) for what reason is the scope and method of personal data processing actually necessary for the realization of the legitimate interests specified in point a; c) what are the rights and freedoms of the data subject that are violated during the processing of personal data; d) how do the legitimate interests of Krediidiregister OÜ and third parties (points a and b) outweigh the interests and fundamental rights of the data subject (point c); We emphasize that the analysis of legitimate interest is primarily intended for data subjects, therefore it must be so clear and understandable that every data subject can understand the necessity of processing personal data when reading the analysis of legitimate interest.

### 3.7. The data protection conditions disclosed on the taust.ee website

The principle of transparency requires that all information related to the processing of personal data is easily accessible, understandable and clearly formulated for the data subject. This primarily concerns the notification of data subjects in order to ensure fair and transparent processing (see Recital 39 of the IKÜM). The notification of people is more precisely regulated by articles 12 - 14 of the General Data Protection Regulation. Given that in a specific case data is not collected from the person himself, the data protection conditions must be based on paragraphs 1 and 2 of Article 14 of the General Data Protection Regulation. In the following, we highlight the shortcomings of the data protection conditions disclosed on the taust.ee website:

- a. Contact details of the data protection officer (IKÜM article 14 paragraph 1 point b) According to the business register, Krediidiregister OÜ has appointed a data protection specialist (Art Andresson, art@taust.ee). There are no contact details of the data protection specialist in the data protection conditions.
- b. Types of relevant personal data (IKÜM article 14 paragraph 1 point d) Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 There is no relevant information in the data protection conditions. All types of personal data that

are processed on the taust.ee website must be listed (including name, personal identification number, valid and invalid connections with a legal entity (how the connections arise), debts). Krediidiregister OÜ must critically review its entire data processing and bring the data protection conditions into line with reality. We also emphasize that the list must be complete and it is not allowed to bring out a sample list. c. Information on receivers and categories of receivers (Article 14, paragraph 1, point e of the General Data Protection Regulation) The data protection conditions must list all receivers, or their categories, to whom personal data may be transferred. Krediidiregister OÜ has stated in the data protection condition: OÜ Krediidiregister may pass on the processing of data to its cooperation partners (authorized processors) with whom a relevant agreement has been concluded and who process the data in accordance with the requirements prescribed by law. Here it remains unclear whether Krediidiregister OÜ has authorized processors to whom personal data is transferred or not. If personal data is transferred to third parties (e.g. accountant, IT support), these companies or categories must also be listed in the terms. In practice, a list of recipients is also used separately from the data protection conditions - that is, the data protection conditions have a reference to a specific web page (file) where it is possible to see the list of recipients. This allows the list of recipients to be changed according to reality, without having to change the data protection conditions. d. Personal data retention period (IKÜM Article 14(2)(a)) There is no personal data retention period or criteria for determining the period in the data protection conditions. A simple reference to the fact that personal data is processed until the goals are achieved is not sufficient or understandable, i.e. it is not possible to understand how long Krediidiregister OÜ stores personal data. In addition, the inspectorate does not agree that Krediidiregister OÜ can store the data of a private person indefinitely. e. If the processing of personal data is based on point f of Article 6, paragraph 1, then information about the legitimate interests of the data controller or a third party (Article 14, paragraph 2, point b of the GDPR) There is no relevant information in the data protection conditions. If the legal basis for the processing of personal data is Article 6(1)(f) of the IKÜM (legitimate interest), then either: 1) the prepared legitimate interest analysis must be added to the data protection conditions, i.e. every person can familiarize himself with the legitimate interest analysis prepared by Krediidiregister OÜ by reading the data protection conditions, or; 2) information that the person has the right to ask for a legitimate interest analysis (e.g. to read the legitimate interest analysis, please send a request to the e-mail address [art@taust.ee](mailto:art@taust.ee)). f. Information on the right to transfer personal data (Article 14(2)(c) of the General Data Protection Regulation) The above information is not included in the data protection conditions. The right to transfer data is regulated in Article 20 g of the IKÜ. Information about the source of the personal data and, in relevant cases, whether it originates from

publicly available sources (Article 14(2)(f) of IKÜM) The data protection conditions provide examples of the sources of data (e.g. business register, land register), i.e. a sample list. It is not legitimate to point out sources of origin in this way. We explain that in general (i.e. addressed to everyone) conditions, the sources where the relevant data are collected must be specified in as much detail as possible. The data protection conditions are missing, for example, court decisions that Krediidiregister OÜ collects and which taust.ee refers to. In a situation where data is collected from sources that cannot be identified in advance in the general conditions (e.g. the name of the creditor), then Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 must be cited in the data protection conditions, that data is also obtained from creditors (when entering a claim). In addition, the data protection conditions (including the name of the creditor) must be forwarded to the data subject either (see IKÜM Article 14 paragraph 3): 1) at the latest when the data subject's personal data (including debt) is first transmitted to a third party, or; 2) upon initial contact with the data subject (e.g. when sending a notice of indebtedness), or; 3) if the above conditions are not met, then within one month of receiving the (contact) data at the latest. In other words, in a situation where Krediidiregister OÜ receives the data subject's contact information (e.g. when entering a claim from a third party), Krediidiregister OÜ has the obligation to provide the data subject with all the information provided for in paragraphs 1 and 2 of Article 14 of the IKÜM (including the name of the person entering the debt, if this is not clearly known to the data subject in advance ). h. Information about the automated decisions referred to in Article 22 paragraphs 1 and 4, including profile analysis, and at least in these cases substantive information about the logic used and what the importance and predictable consequences of such personal data processing are for the data subject (Article 13 paragraph 2 point f). The data protection conditions state that profiling is carried out on the basis of OÜ Krediidiregister's legitimate interest. At the same time, there is no substantive information about the logic and what are the importance and predictable consequences of such personal data processing for the data subject (see also recital 60 of IKÜM). i. The taust.ee website uses third-party cookies (e.g. Google analytics), but there is no information about this in the data protection conditions. We explain that in the situation where Krediidiregister OÜ installs third-party cookies on its website, Krediidiregister OÜ is the responsible processor in this regard, and Krediidiregister OÜ must have a specific legal basis for installing cookies. In this regard, Article 5(3) of Directive 2002/58 on privacy and electronic communications states the following: Member States shall ensure that the storage of information in a subscriber's or user's terminal device and access to information already stored therein is permitted only under the condition that the relevant subscriber or user has given his consent, and he has been provided with clear and

comprehensible information in accordance with Directive 95/46/EC, including the purpose of data processing. This does not prevent the technical storage or access of data, the sole purpose of which is to transmit communication in an electronic communication network or which is essential for the service provider to provide such an information society service that the subscriber or user has explicitly requested. Given that there are no more precise rules regarding the use of cookies in Estonia, the requirements of the said directive must be followed. At the same time, the directive explicitly stipulates that the prior consent of the person must be obtained for the use of cookies, except in cases where the sole purpose of the technical storage and access of data is to transmit communication in an electronic communication network or which is essential for the service provider to provide an information society service. The obligation to consent has also been confirmed by the European Court on 01.10.2019 in case number C-673/173. In the decision, the European Court has also emphasized that consent to the use of third-party cookies must be obtained regardless of whether it is personal data or not.

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=984162> Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 Therefore, the use of third-party cookies on the taust.ee website is illegal in this case, and such processing must be stopped until the person's consent to the use of cookies in accordance with Article 7 of the IKÜM is obtained. Also, the consent must be voluntary, i.e. the person must be able to decide for himself the use of third-party (and not essential) cookies. Based on the above, the data protection conditions disclosed on the taust.ee page do not meet the requirements set forth in the IKÜM (Article 5(1)(a), Article 12(1) and Article 14(1) and (2) of the IKÜM). SUMMARY: Considering the above, the data processing on the taust.ee website does not comply with the principles stated in article 5, paragraph 1 of IKÜM. If the processing of personal data does not comply with the principles set forth in Article 5 of the IKÜM, the processing of personal data is prohibited. The data processor himself is responsible for the fulfillment of these principles and must prove their fulfillment (see IKÜM Article 5 paragraph 2). Therefore, the taust.ee website must stop processing the personal data of natural persons (including representatives of legal entities) until the processing of personal data is brought into full compliance with the requirements of IKÜM. Pursuant to § 58 (1) of the Personal Data Protection Act and Article 58 (2) d and f of the General Regulation on Personal Data Protection, the inspectorate has the right to order that the data controller bring personal data processing operations into compliance with IKÜ requirements in a certain way and within a certain period of time, and the right to establish temporary or permanent personal data processing restriction, including a processing ban. Taking into account the

factual circumstances and the fact that in a specific case, personal data is processed illegally on the website [www.taust.ee](http://www.taust.ee) (the data processing does not meet the requirements set forth in Articles 5, 6, 7, 12 and 14 of the IKÜM), the inspection considers that the mandatory injunction taking action in this matter is necessary to end the offense as soon as possible. /signed digitally/  
Raiko Kaur lawyer under the authority of the Director General