PRIVACY PROTECTION AND STATE TRANSPARENCY Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 PRESCRIPTION-WARNING in personal data protection case no. 2.3.-3/17/1565 Prescription author Raiko, a lawyer at the Data Protection Inspectorate Kaur Time and place of making the injunction 09.03.2022, Tallinn Addressee of the injunction responsible person Äripäev AS (10145981) firma@aripaev.ee Representative: Advokaadibüroo TRINITI OÜ maarja.pild@triniti.ee Board member RESOLUTION: Section 56 of the Personal Data Protection Act (IKS) 1, subsection 2 point 8, § 58 subsection 1 and Article 58 subsection 1 point d and subsection 2 point d of the General Personal Data Protection Regulation (GPR), as well as taking into account articles 5, 6, 7, 12 and 14 of the General Regulation on Personal Data Protection (GPR), the Data Protection Inspectorate makes Äripäev AS mandatory injunction to comply with the website www.infopank.ee: 1. Limit the period of disclosure of former board members and members of the supervisory board to five years in general (see point 3.1 of the Data Protection Inspectorate's reasons); 2. Stop enabling searches by name of a natural person on the website, if the natural person does not have a valid business relationship with a specific organization (see point 3.1 of the Data Protection Inspectorate's reasons); 3. To stop processing personal data of other related persons on the website (including transmission, disclosure) (see point 3.2 of the reasons of the Data Protection Inspectorate); 4. End the search engine indexability of the website through personal data (including the name of the representative) (see point 3.3 of the reasons of the Data Protection Inspectorate); 5. Stop using third-party cookies on the website until the person's consent to use cookies is obtained in accordance with Article 7 of the General Data Protection Regulation (see point 3.4 of the Data Protection Inspectorate's reasons); 6. Bring the data protection conditions into line with the requirements set forth in articles 12 and 14 of the Data Protection Inspectorate (see point 3.5 of the Data Protection Inspectorate's reasons) Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 We set the deadline for the fulfillment of the injunction to be 30.03.2022 .a. Report compliance with the order to the e-mail address of the Data Protection Inspectorate at info@aki.ee by this deadline at the latest. REFERENCE FOR DISPUTES: You can contest this order within 30 days by submitting either: - an appeal in accordance with the Administrative Procedure Act to the Data Protection Inspectorate or - an appeal in accordance with the Administrative Court Procedure Code to the Tallinn Administrative Court (in this case, the appeal in the same matter cannot be reviewed). Challenging a precept does not stop the obligation to fulfill it or the implementation of measures necessary for fulfillment. EXERCISE MONEY WARNING: If the injunction has not been complied with by the specified deadline, the Data Protection Inspectorate will assign the addressee of the injunction to the recipient of the injunction on the

basis of § 60 of the Personal Data Protection Act: Extortion money for each unfulfilled injunction point of 20,000 euros. 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. FACTUAL FACTS: On 25.07.2017, the Data Protection Inspectorate (inspection) started a self-initiated monitoring procedure (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 Äripäev AS 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 is to check compliance with the requirements set forth in the Personal Data Protection Act. In connection with the ongoing supervision procedure, we carried out an additional analysis in the light of IKÜM and forwarded to Äripäev AS 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 proposal of 01.06.2020, we pointed out, among other things, that it is prohibited to find a web page in an indexable way for search engines through personal data, and that data protection conditions must be drawn up and disclosed, which fully meet the requirements set forth in Articles 12 - 14 of the IKÜM. Äripäev AS has confirmed as part of the supervision procedure that it has brought its activities into line with the requirements set out in Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 IKÜM. However, Äripäev AS has not finished indexing the web site through personal data and has also submitted an objection in this regard on 21.10.2020. On 22.02.2022, the inspectorate made proposals to

gain access to the website www.infopank.ee and to obtain a legitimate interest analysis, and on 03.03.2022 Äripäev AS fulfilled the proposals of the inspectorate. 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 supervision 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 then their disclosure on the website www.infopank.ee (hereinafter also infopank.ee or infopank). The Data Protection Inspectorate checked the compliance of the website infopank.ee with the principles of personal data processing (Article 5 paragraph 1 of IKÜM) as part of the supervision procedure. Äripäev AS was responsible for proving compliance with IKÜM requirements (Article 5 paragraph 2 of IKÜM), therefore 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 infopank.ee website. 1.1. Processing of personal data on the infopank.ee website The Inspectorate logged in to the infopank.ee website in order to see the view of the logged-in and paid user (hereinafter the user). The user can make inquiries on the website by company name and registry code, as well as by the name 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 comes up: 1.1. Information card - the executive management team (name, connection since, connection with the company (e.g. board member), position (e.g. financial director, chairman of the board), area of responsibility (e.g. finance, management) and former members of the executive management team (name, connection with the company, period) are displayed. 1.2. Business connections - executive management, members of the council (name, relationship from, relationship with the company, position (e.g. chairman of the council), owners (name, relationship from,

percentage, participation (amount)) are displayed, other related persons (name, relationship with the company (e.g. employee), occupation (e.g. group marketing manager, spokesperson, director of administration, chief inspector), area of responsibility (e.g. public relations, marketing, administration) and historical connections in the spider of connections (names of people). 1.3 Business analytics - it is possible to buy company credit reports that include responsible persons (board) and others related persons (owner, members of the supervisory board, founder, auditor). From the sample report, Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 shows that the company is also displayed persons previously associated with the company (name, personal identification number, relationship with the company (board member, partner) and period. 2. It is then possible to open each natural person (both past and present relationships) separately. It is also possible to do this as a separate search based on the name of a specific natural person. The identity card of a natural person displays: 2.1. Information card 2.1.1. General information - date of birth and age, social security number, gender. 2.1.2. Contacts - e-mail, telephone and reference to where the data was obtained (e.g. contacts of a specific company); 2.1.3. Board member in companies (list of organizations, connection to the company, occupation); 2.1.4. Ownership (names of organizations, percentage and participation (in sum); 2.1.5. Tenure (time (e.g. 2015-2017), company name, role/title (e.g. board member), area of responsibility); 2.2. Business relationships (see content in point 1.2) Based on from the above, personal data is processed on the infopank.ee website, which must be based on the requirements set out in the Personal Data Act. Äripäev AS has explained that personal data is processed on the basis of legitimate interest. Legitimate interest analyzes have also been submitted to the inspection. 2. Principles of personal data processing The personal data processor is obliged to follow the principles set forth in Article 5, Paragraph 1 of the GDPR. The controller himself is responsible for the fulfillment of these principles and must be able to prove their fulfillment (see Article 5, Paragraph 2 of the GDPR). To the extent that data processing does not fully comply with the principles stipulated in Article 5, Paragraph 1 of the GDPR, data processing is prohibited. In the proposal of 01.06.2020, we outlined the mandatory principles of personal data processing and explanations regarding them: - Legality, fairness and transparency (IKÜM article 5 paragraph 1 point a) Any processing of personal data must be fair and legal, i.e. in full compliance with all valid legislation (including IKÜM and 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). Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 - Purpose and storage 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. Thus, the information portal has an obligation to ensure the correctness of all processed personal data (e.g. violation of previous contractual obligations, amounts 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. 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 evaluate the compliance of data processing at infopank.ee with the principles of personal data processing. 3. Compliance with IKÜM requirements 3.1. Disclosure of former members of the executive management The info card of the Infopank.ee

website lists the members of the former executive management (name, relationship with the company, period). During the spot check, we identified a situation where one company has had one board member continuously since 06.01.2015. However, the same board member has been included under the former board member of the same company and the period (07.01.2015 – 09.12.2017) has also been added. In this case, it remains unclear whether and on the basis of which Äripäev AS adds board members to the category of former board members or why such an error has occurred. Regarding the deadline for disclosure of data of former members of the executive management, Äripäev AS has noted the following in its analysis of the legitimate interest in publishing and keeping historical information: From the perspective of the company: The background cards of the company show the history of the members of the management board and the supervisory board up to 10 years (relationships older than 10 years are removed from the company's information cards). Namely, 10 years is the maximum statute of limitations for civil law claims (in certain very exceptional cases, the statute of limitations also reaches 30 years, but Äripäev should be based on 10 years) and therefore it is important for the overall picture to keep the data as long as civil claims can be submitted in connection with the circumstances in which the relevant person was still part of the management. In person view: In the person view, the entire business CV of the person is critically indicated. If it is arbitrarily interrupted at a certain point, it does not convey the whole picture. The Inspectorate remains incomprehensible, based on which Äripäev AS considers that the statute of limitations for claims against the members of the management board and the members of the supervisory board is 10 (30) years. The Commercial Code regulates the statute of limitations for claims against the persons in the aforementioned position, which is generally five years (see ÄS § 315(3) and § 327(3)). Based on this, the inspectorate is also of the opinion that the history of the members of the executive management can be made public for up to 5 years on the basis of legitimate interest. The inspection does not rule out that in certain cases it may be necessary to disclose historical data for a longer period of time, but this requires an assessment based on the specific case. In addition, according to the inspection, it must be distinguished whether the person whose data is disclosed on the website has a valid connection with a legal entity or not. If a person does not have a valid business relationship with any legal entity, enabling a search by name of a natural person on the infopank.ee website is redundant. In the opinion of the Inspectorate, there is no legitimate purpose that would justify making inquiries about a natural person in such a case. If a person has a specific claim against a former member of the board of a particular legal entity, he can get this information by looking at the data of the legal entity - i.e. by entering the name of the organization in the search on the infopank.ee website, you can also see the former members of the board and the period of

their membership. 3.2. Disclosure of other persons related to the organization On the Infopank.ee website, other related persons are listed under business connections. In their case, the name, connection with the company, occupation, area of responsibility are indicated. In addition, it is possible to open these persons in the information bank and see the person's contact details (e-mail, telephone). During the spot check, we found that, for example, employees of a specific organization are added under other persons, probably the occupation of a specific employee is taken into account when making a decision. For example, we identified employees with the following positions - group marketing manager, press representative, administration director, chief inspector. It remains unclear on the basis of which Äripäev AS decides that it is legal to re-(disclose) the data of these employees. In addition, in the analysis of the legitimate interest of the information bank, it is stated that the information bank only has data on persons involved in business activities. However, this information is not true - employees who work in a specific organization cannot automatically be considered as persons related to business activities (including, for example, public sector employees). In addition, we found that on the infopank.ee website, under persons related to the organization, there are persons who in fact no longer have anything to do with this organization, and the positions of the employees have also changed. In other words, false information has been published on the infopank.ee website, which is prohibited due to the IKÜM. During the check, we identified, for example, one organization whose data was last updated on 20.02.2020 and another whose data was updated on 30.08.2021. Based on the above, we consider that the selection of key employees is speculative (ie Äripäev AS cannot assess whether it is an employee who can influence the (business) activities of a specific legal entity). It is also not possible to guarantee the correctness of the data when (re)publicizing the data - the exchange of employees' workplace/position and contact information can take place at any time. However, if it is not possible to ensure the correctness of the data, data processing is prohibited, regardless of the legal basis. Therefore, Äripäev AS must stop processing data of other related persons in the information bank (including transmission, disclosure). 3.3. Search engine indexability of the web page through personal data (including name) The web page www.infopank.ee is indexable by search engines through personal data (the name of a natural person). By entering, for example, a person's first and last name in the Google search engine, the information published by Äripäev AS about legal entities related to it, including non-profit organizations, will appear clearly and by name in the Google search results: XXX Äripäev AS has sent on 20.10.2020 explanations of why indexing is important, including pointed out that indexing serves the Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 purpose of helping to maintain and create an open society. The Inspectorate agrees with the stated

purpose, but this does not mean that the discovery of the infopank.ee website through personal data can be legitimate for such a purpose. This goal can also be fulfilled if legal entities (company name/registration code, etc.) and not personal data are indexed. The following are the reasons why indexing through personal data is not allowed in the opinion of the inspectorate: - In a situation where personal data (e.g. the name of a natural person) is entered into the search engine, there is a very high probability that the information will be searched for a specific natural person (e.g. his contact details, social networks, i.e. data, which the data subject shows about himself as a natural person), not legal entities and related information. At the same time, Äripäev AS cannot in any way guarantee that the release of data (e.g. related companies, availability of information in Äripäev's information bank) is necessary for the searcher (fit for purpose); - According to the inspection, the purpose of indexing the name of a natural person is to advertise the service and thereby get a customer and/or sell a service to him. Although Äripäev AS has stated: Äripäev does not agree that the purpose of indexing is advertising - adding a link to Infopank through information in a search engine is rather similar to an encyclopedia based on a keyword, a road, a road reference list or an otogu search system of the library library.e, the inspection does not agree with such a comparison. An information bank whose business is the sale of (personal) data and, therefore, the desire for the highest possible number of visitors to the website, is not comparable to an encyclopedia or a library search system. In addition, it is possible to advertise your service without personal data, just like any other service. If the person has landed on the service provider's page as a result of advertising, he can also be offered the opportunity to make inquiries about the members of the executive management on the website. - Displaying associations of non-profit organizations, including apartment associations, in the results of the search engine by name allows to draw conclusions about a person's place of residence and other private life circumstances in a simple way (e.g. membership in an association engaged in a certain hobby, an association of people suffering from a certain disease). Disseminating such information to everyone indiscriminately cannot be a legitimate interest of AS Äripäev. - Over the years, the inspectorate has received the most complaints about the fact that information about a person is in the results of an internet search engine. In other words, this is what bothers people the most, it is perceived as the greatest invasion of privacy. - The operator of the Internet search engine is a separate responsible data processor who can be requested to remove data. However, this does not justify the data discloser disclosing the data in such a way that it can be indexed by search engines. Disclosure of personal data in this way increases the invasion of privacy and clearly tilts the scale of legitimate interest to the detriment of the person. The default option that all people's data is made public in an indexable manner (essentially thrown on

the internet) cannot be considered suitable, and each person must start submitting requests to the operators of internet search engines to eliminate this consequence. 3.4. Use of third-party cookies We explain that in a situation where Äripäev AS installs third-party cookies on its website, Äripäev AS is the responsible processor in this regard, and there must be 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 in accordance with Directive 95/46/EC, he has been provided with clear and understandable information, among other things, about the purpose of processing the data Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235. 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-673/171. 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. Even if it were to come to the conclusion that the aforementioned directive is not directly applicable, Äripäev AS is obliged to follow the requirements set forth in IKÜM. The website www.infopank.ee collects various cookies, including Google Analytics cookies. IKÜM derives from Recital 30: Natural persons can be associated with network identifiers shared by their devices, applications, tools and protocols, such as IP addresses or cookies. This may leave traces that may be used to profile and identify natural persons, in particular when combined with unique identifiers and other information arriving at the servers. Therefore, the use of cookies is also clearly the processing of personal data, and for this a legal basis is required, which in established practice in Europe can only be the consent of the data subject. The data subject must understand which cookies the website collects and must be able to give separate consent for each type of cookie (except for cookies that are essential for the website to function). Therefore, the use of third-party cookies on the infopank.ee website is illegal in this case, and such

processing must be stopped until the person's consent in accordance with Article 7 of the IKÜM is obtained for the use of cookies. Consent must also be voluntary, i.e. the person must be able to decide for himself the use of third-party (and not essential) cookies - this means that cookies must not be installed until the person gives permission for this. 3.5. Data protection conditions (including the register of processing operations) The principle of transparency requires that all information related to the processing of personal data is easily accessible, understandable and clearly worded to 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). Notifying people is more precisely regulated by articles 12 - 14 of the General Data Protection Regulation. Considering 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. Äripäev AS has published the data protection conditions, including the register of processing operations, on the infopank.ee website. In the following, we highlight the deficiencies in the data protection conditions disclosed on the infopank.ee website (including the register of processing operations): a. Types of relevant personal data (IKÜM Article 14(1)(d)) Not all types of personal data are correctly listed in the register of processing operations. Namely, there are no types such as personal identification number, date of birth, age, gender. Although these data fields are listed in the register, only where they concern the recipients

Äripäev AS's own employees. At the same time, the user of the Äripäev AS information bank can also get acquainted with the above information. b. Period of storage of personal data (IKÜM Article 14(2)(a)) It follows from the register of processing operations that all personal data is stored indefinitely on the infopank.ee website. However, in the analysis of the legitimate interest in the publication and storage of historical information submitted to the inspection, it is indicated that the company's background cards show the history of the board and council members for up to 10 years. Although both indefinite and 10-year data disclosure time are excessive in the opinion of the inspectorate (see point 3.1. of the inspectorate's reasons), both the legitimate interest analysis and the data protection conditions must still be in accordance. c. Information on the right to object to the processing of personal data (Article 14, paragraph 2, clause 2 of the Data Protection Act does not contain the above information. The right to object is more precisely regulated in Article 21 of the Data Protection Act. We explain that the data subject has the right to object to the processing of personal data concerning him at any time based on his specific situation,

which takes place on the basis of a legitimate interest. d. Information about the source of origin of personal data and, in relevant cases, whether they originate from publicly available sources (Article 14, paragraph 2, point f of IKÜM) It is stated in the register of processing operations that the source of data is lexicons. The inspection remains unclear as to which lexicons are taken into account during data collection. However, the sources of origin of data collection must be as clear and understandable as possible. e. Information about the automated decisions referred to in paragraphs 1 and 4 of Article 22, including profile analysis, and at least in these cases the substantive information used a logic and what are the importance and predictable consequences of such personal data processing for the data subject (Article 13(2)(f) of the GDPR) The data protection conditions only list examples for which automatic decisions are made. We explain that the data protection conditions must state all information regarding automated decision-making, including profile analysis. There is also no substantive information in the conditions about the logic and the importance and predictable consequences of such personal data processing for the data subject (see also paragraph 60 of the IKÜM). Based on the above, the data protection conditions disclosed on the infopank.ee page (including the register of processing operations) do not meet the requirements set forth in IKÜM (ICÜM Article 5(1)(a), Article 12(1) and Article 14(1) and (2)). SUMMARY: Considering the above, the data processing on the infopank.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 processing of personal data on the website infopank.ee must be brought into line with the requirements of the IKÜ without delay. According to § 58 subsection 1 of the Personal Data Protection Act and Article 58 subsection 2 point d of the General Regulation on Personal Data Protection, the inspectorate has the right to order that the data controller transfer to Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 personal data processing operations in a certain way and within a certain period of time comply with the requirements of IKÜM. Taking into account the factual circumstances and the fact that in a specific case personal data is processed on the website www.infopank.ee illegally (data processing does not comply with the provisions of articles 5, 6, 7, 12 and 14 of IKÜM requirements), the inspectorate considers that issuing a mandatory injunction in this case is necessary in order to end the offense as soon as possible. /signed digitally/ Raiko Kaur lawyer under the authority of the Director General