

PROTECTION OF PRIVACY AND TRANSPARENCY OF THE STATE Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 PRECAUTIONS-WARNING in personal data protection matter no. 2.1.-6/21/20 Preceptor of the Data Protection Inspectorate Raiko Kaur Time and place of precept 23.07.2021, Tallinn Addressee of precept Penteer OÜ (10141537) penteer@concept2.ee Responsible person Member of the Management Board RESOLUTION: § 56 (1), (2) (8), § 58 (1) of the Personal Data Protection Act and Pursuant to Article 58 (1) (d) and (e) and (2) (d) and (f) of the General Data Protection Regulation (IKÜM), and also taking into account Articles 5, 6, 12 and 13 of the IKÜM, the Data Protection Inspectorate shall issue a mandatory precept to Penteer OÜ: -I collection of copies of customers' identity documents (see point 2 of the recitals of the Data Protection Inspectorate and its sub-points); 2. Add to the concept2.ee website data protection conditions that fully comply with the requirements set out in Articles 12 - 13 of the CISA (see Section 3 of the recitals of the Data Protection Inspectorate for the existing shortcomings). Also send a copy of the data protection conditions attached to the website to the Inspectorate (in PDF or Word format). We set the deadline for compliance with the precept as 13.08.2021. Notify the Data Protection Inspectorate to the e-mail address info@aki.ee of the fulfillment of the precept by the deadline. CONTEST REFERENCE: This precept can be challenged within 30 days by submitting either: - a challenge under the Administrative Procedure Act to the Data Protection Inspectorate, or - an appeal to the Tallinn Administrative Court under the Code of Administrative Court Procedure (in which case the challenge can no longer be heard). Contestation of a precept does not suspend the obligation to comply with the precept or the application of the measures necessary for compliance. PENALTY WARNING: If a precept is not complied with by the specified deadline, the Data Protection Inspectorate shall impose a penalty payment on the addressee of the precept on the basis of § 60 of the Personal Data Protection Act for each item of the precept not complied with. The penalty payment may be imposed repeatedly - until the precept is complied with. If the addressee does not pay a penalty payment at Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235, it shall be forwarded to a bailiff for the commencement of enforcement proceedings. In this case, the bailiff's fee and other enforcement costs are added to the penalty payment. WARRANTY PENALTY WARRANTY: Misdemeanor proceedings may be instituted for failure to comply with a precept pursuant to Article 58 (1) of the General Data Protection Regulation on the grounds of § 70 of the Personal Data Protection Act. A natural person may be fined up to EUR 20 000 000 for this act and a legal person may be fined up to EUR 20 000 000 or up to 4% of its total annual worldwide turnover, whichever is greater. The Data Protection Inspectorate conducts extra-judicial proceedings against misdemeanors. FACTUAL FACTS: On 26.03.2021,

the Data Protection Inspectorate (Inspectorate) received an application in case number 2.1.-1/21/1243, according to which Penteer OÜ requests a copy of an identity document for concluding a lease agreement and only a digital signature is not suitable for concluding an agreement. The person's request was also clearly not answered. If the person wanted to know what a copy of an identity document is required and why only a digital signature is not suitable, then the answer was: We ask for a copy of the document, because we have such a procedure in place in the company. The contract was refused because the person did not provide a copy of the identity document. In addition, the person wanted to see the data protection conditions that comply with Articles 13 to 14 of the General Data Protection Regulation, but also in this respect the person was not answered. Based on the above, we initiated an own-initiative monitoring procedure. On 28.04.2021, we made a proposal and inquiry to Penteer OÜ with the following content: To prepare and submit to the Inspectorate the data protection conditions added / to be added to the website concept2.ee, which fully comply with the requirements set out in Articles 12 - 14 of the CISA. Reply to the proposal no later than 12.05.2021. In addition, the Data Protection Inspectorate has the right to request explanations and other information, including the submission of documents necessary for conducting supervisory proceedings¹, therefore please submit the following information no later than 12 May 2021: if a person digitally signs a lease and doesn't use a postpaid service? 1.1. If there is no such need and OÜ Penteer terminates the collection of a copy of identity documents in the cases specified in clause 1, confirm it. 1.2. If so, however: - on what legal basis is a copy of an identity document made? - explain in a thorough and comprehensible manner the necessity (purposefulness) of a copy of an identity document, including why it is not possible to limit the fulfillment of a specific purpose or goals by using less intrusive measures (incl. why a digital signature is not enough)? The representative of Penteer OÜ forwarded the data protection conditions and the position according to which 1 Legal basis for requesting explanations: in case of non-administrative persons § 30 (1) and (3) of the Law Enforcement Act together with Article 58 (1) a) and e) of the General Data Protection Regulation; in the case of an administrative authority pursuant to § 752 (1) (1) of the Government of the Republic Act Collection of a copy of an identity document of Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee On 19.05.2021, the Inspectorate sent a repeated proposal, in which we also provided explanations of why the collection of a copy of an identity document is not justified. In addition, we highlighted the most important shortcomings that we identified during the review of the data protection conditions. Based on this, we made the following proposals: 1. To stop collecting copies of the identity documents of OÜ Penteer's customers; 2. To compile and submit to the Inspectorate the data protection conditions added / to be added to the website

concept2.ee, which fully comply with the requirements set out in Articles 12 - 14 of the CISA. Answer the proposal no later than 02.06.2021.

EXPLANATION OF THE PERSONAL DATA PROCESSOR

In response to AKI's proposals, the Client announces the following:

1. The Client agrees with AKI's position that in a situation where a person digitally signs a contract, it is generally not necessary (unless required by special law) to collect additional copies of an identity document. In this case, it is not really necessary to submit an identity document in order to enter into an agreement, and the Client agrees to change the principles of personal data processing in this regard. At the same time, it is necessary to take into account the fact that the Client often concludes lease agreements for sports equipment in paper form, which agreement is signed by the parties by hand - in this case the Client has the right to establish his / her identity before concluding the lease. In this regard, the AKI has also correctly indicated that in this case or the collection of additional data may be necessary. The Customer also has the right and obligation to establish the identity of its customer at the moment when the customer accepts direct possession of the leased sports equipment - the Customer has the obligation to ensure that the object is handed over to the person specified in the lease, but not to any person. There is a frequent case law where a person named as a party to a contract claims that he has not signed the contract (especially in the case of paper-based contracts) or that he has not received any item under the contract. In such a case, the burden of proving the Client is to prove the opposite, ie that the contract has been entered into and the object has been received by the person specified in the lease agreement. The existence of a copy of an identity document is in this case one of the most important pieces of evidence, which proves that the Client has been visited by the person specified in the lease agreement, but not by any person. Pursuant to Article 6 (1) of the General Regulation on the Protection of Personal Data (hereinafter: EDPS), the processing of personal data is lawful only if at least one of the following conditions is met and to the extent that: (a) for a specific purpose; (b) the processing of personal data is necessary for the performance of a contract concluded with the participation of the data subject; (c) the processing of personal data is necessary for the legitimate interests of the controller or of a third party, unless such interests outweigh the interests or fundamental rights and freedoms of the data subject for the protection of personal data, in particular where the data subject is a child. The Client emphasizes that making a copy of an identity document (ie in the case of a paper lease and upon receipt of an object) will only take place if the data subject has given his or her consent. If the Client refuses to give his consent, a copy of the identity document will not be made, but in this case the Client has the right to refuse to enter into a lease agreement due to the principle of freedom of contract. In view of the above, the processing of personal data (ie making a copy of an identity document) is lawful and permissible under

Article 6 (1) (a) of the ECHR. Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 On the basis of the concluded lease agreement, the Customer is obliged to ensure that the leased object is handed over to the person specified in the lease agreement (not to any person). (ie making a copy of an identity document) is also legal and permissible under Article 6 (1) (b) of the CISA, ie for performance under a lease. The processing of personal data (ie making a copy of an identity document) is also necessary in this case to fulfill the above-mentioned burden of proof on the Client, therefore the processing of personal data (ie making a copy of an identity document) is also legal and permissible under Article 6 (1) (f). In conclusion, the Client is of the opinion that the Client has the right to make a copy of his / her client's identity document upon concluding a lease agreement in paper form and transferring direct possession of the leased object to his / her client, provided that the data subject has given his / her consent. 2. In connection with the preparation of data protection conditions complying with the requirements of Article 12-14 of the CISA, the Client requests to announce in advance the final opinion of the CCP on the Client's opinion, after which the Client can finalize the respective data protection conditions and submit them to the CCI

GROUND FOR THE DATA PROTECTION INSPECTORATE: 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 identified, directly or indirectly, in particular by reference to an identifier such as a name, a personal identification number (see Article 4 (1) of the CISA). Personal data is also a picture of a person. According to the materials of the case, Penteer OÜ wishes to continue making a copy of the customer's identity document if the lease agreement is entered into in paper form and if the possession of the leased object is transferred. Considering that the identity document contains, for example, a person's name, personal identification code, picture, the collection and storage of a copy is a processing of personal data. 2. Legal basis for the processing of personal data The processing of personal data is lawful only if at least one of the conditions set out in Article 6 (1) of the General Regulation on the Protection of Personal Data (EDPS) is fulfilled. Penteer OÜ considers that the legal bases for the collection and storage of identity documents are consent, a contract and a legitimate interest (Article 6 (1) (a), (b) and (f) of the CISA). In doing so, we emphasize that the processing of personal data must be lawful and the burden of proof lies with the data controller (see Article 5 (1) (a) and Article 5 (2) of the CISA). 2.1. Consent The representative of Penteer OÜ responded to the consent as follows: The Client emphasizes that making a copy of an identity document (ie in the case of a paper lease and acceptance of an object) only takes place if the data subject has given his or her consent. If the Client refuses to give his consent, a copy of the identity document will not be made, but in this case the Client has the right to refuse to enter

into a lease agreement due to the principle of freedom of contract. In view of the above, the processing of personal data (ie making a copy of an identity document) is lawful and permissible under Article 6 (1) (a) of the ECHR. Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 We repeat here the proposal of 19.05.2021: We explain that in a situation where the transfer of data for the use of equipment is mandatory, ie the service cannot be used without the transfer of data, there can be no data processing on the basis of consent within the meaning of the IORP. Consent can only be used as a basis for the processing of personal data in cases where the processing of personal data (including collection) is not unavoidable and the person can really decide whether or not he or she wishes to give consent. Failure to give consent must not have negative consequences. In other words, with consent, it should be possible to use the service without transferring data. The use of consent is possible, for example, in a situation where a person can decide at the time of making a purchase whether or not to give consent to receive offers, and regardless of whether consent has been given, it is possible to continue making the purchase. However, it is wrong to ask for consent in a situation where there is in fact another legal basis for the processing of personal data, ie whether or not consent is given, the processing of the data is still necessary for the data controller. In the specific case, there is no voluntary consent within the meaning of the IKÜM, taking into account that in a situation where a copy of an identity document is not forwarded, it is not possible to enter into an agreement with Penteer OÜ. With regard to consent, we recommend that you also read the conditions for granting consent set out in the CISA (Article 7 of the CISA) as well as the general instructions for the processor of personal data prepared by the Inspectorate (Chapter 9. Requesting consent; Appendix 2. Consent checklist).

2.2. Agreement The representative of Penteer OÜ replied as follows regarding the agreement: Based on the concluded lease agreement, the Client is obliged to ensure that the leased object is handed over to the (not random) person specified in the lease agreement. 6 (1) (b), ie for performance under a lease. The Data Protection Inspectorate does not agree with the position of the representative of Penteer OÜ. We explain that the company has the right to ask customers for essential personal data (name, personal identification code, contact information) and to check the customer's identity. In order to establish identity, it is also possible to ask for an identity document and view it for verification. However, on the basis of the agreement, data processing is limited to the above, ie the identity is established by viewing the document and comparing the image on the document and the customer. However, making and keeping a copy of an identity document can no longer be necessary for the performance of the contract, and the legal basis for such activities can arise from a special law (eg § 21 of the Money Laundering Prevention and Terrorist Financing Act). In particular, we

recommend that you read the instructions prepared by the Inspectorate on legitimate interest in the processing of data under the agreement (Chapters 3.1, 3.2 and 3.3) 2.3. Legitimate interest The processing of personal data (ie making a copy of an identity document) is also necessary in this case to fulfill the above-mentioned burden of proof on the Client, therefore the processing of personal data (ie making a copy of an identity document) is legal and permissible under Article 6 (1) (f).

According to the Supervision Authority, Penteer OÜ has not proved, ie submitted a credible analysis of legitimate interests, that it has a legitimate interest in collecting a copy of its customers' document. Therefore, Penteer OÜ has no legal basis for collecting copies of identity documents. However, if the collection of data at Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 has been illegal, these data may not be used to fulfill the burden of proof. The Inspectorate agrees that identification and subsequent verification is important, but we emphasize that the collection and storage of data for identification purposes must be kept to a minimum. In order for the Inspectorate to be able to assess whether and to what extent data may be collected and stored, Penteer OÜ must perform a thorough analysis of legitimate interests. Alternative measures should be considered and, in the absence of other and less intrusive measures to prove that a particular person has entered into a contract or accepted an object, a copy of the identity documents could be considered. However, the Inspectorate considers that collecting a copy of identity documents from all (paper) parties and recipients of equipment is in any case excessive and it should be sufficient for the data controller to verify the identity and image of the document and, for example, to record the document number. It should be noted that the registration of a document number is also used in many other areas, and the obligation and need to collect a copy of an identity document arises only in special cases and when such an obligation is provided by law. However, if Penteer OÜ finds that there are no alternative and sufficiently effective measures for collecting a copy of an identity document to fulfill its objectives, a correct analysis of legitimate interest must be submitted to the Supervision Authority. However, it is not clear from the answers submitted to the Inspectorate why it is necessary to make a copy of the identity documents and alternative measures (eg fixing the document number) are not sufficient. The interests or fundamental rights and freedoms of the data subject, which may be violated during the collection and storage of identity documents, have also not been assessed, and it has not been considered whether the legitimate interests of Penteer OÜ outweigh the interests of the data subject. We clarify that, according to Article 6 (1) (f) of the CISA, the processing of personal data is lawful if the processing is necessary in the legitimate interest of the controller or of a third party, unless such interests outweigh the interests or fundamental rights and freedoms of the data subject. personal data

must be protected (Article 6 (1) (f) CCIP). Thus, Article 6 (1) (f) of the CISA lays down three conditions, all of which must be satisfied in order for the processing of personal data to be authorized: - the controller or third parties have a legitimate interest in the processing; - the processing of personal data is necessary for the pursuit of a legitimate interest; - the legitimate interests of the controller and / or a third party outweigh the interests, fundamental rights and freedoms of the data subject being protected; The possibility of using this legal basis and its assessment can be divided into three stages, ie firstly the legitimate interests and weight of the data controller or third parties, secondly the rights and interests of the data subject and thirdly the consideration of conflicting interests, including preliminary assessment + additional safeguards and final assessment. In the light of the above, the controller has an obligation to weigh the legitimate interests of himself and / or the third party against the interests and fundamental rights of the data subject, as a result of which Article 6 (1) (f) CISA can be invoked as a legal basis for processing. The fact that the processor has a legitimate interest in the processing of personal data does not automatically mean that the processor can rely on Article 6 (1) (f) of the CCIP. The legitimacy of the controller's interest is only a starting point, ie one of the elements to be analyzed, and whether the basis of a legitimate interest can be relied on depends on the outcome of the balancing act. It is the task of the chief processor to make sure that the provision of a legitimate interest can be relied on, who must carry out the weighing in a transparent manner at Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 justify (prove). Thus, in order to understand whether personal data can be processed on the basis of Article 6 (1) (f) of the CISA, Penteer OÜ must prove whether and what is the legitimate interest of the company. Legitimate interests must be sufficiently clear. This requires a real and present interest - something related to an ongoing activity or a benefit that is expected to accrue in the near future. In other words, interests that are too vague and speculative are not enough. If legitimate interests are not sufficiently clear, these interests cannot be balanced against the interests and fundamental rights of the data subject. It is therefore important that the legitimate interest is in accordance with the applicable law, is sufficiently clear (ie sufficiently specific) and real and current (ie not speculative). Processing on the basis of a legitimate interest must be genuinely necessary, and consideration must be given to whether alternative and less harmful measures can be used to achieve the purpose. Secondly, it is necessary to analyze the possible interests or fundamental rights of the data subject - and the freedoms that may be affected by the processing of personal data. Third, the legitimate interests of Penteer OÜ must be balanced with the interests and fundamental rights of the data subject. The potential impact of the processing (collection, storage) of personal data on the data subject is compared with the legitimate

interests of the controller and it is assessed whether and to what extent the legitimate interests of the controller outweigh the interests of the data subject. If the processor fails to carry out one of the preceding steps correctly, the processing of the data shall not be permitted under Article 6 (1) (f) of the CISA. In particular, we recommend that you also read the instructions on legitimate interests prepared by the Inspectorate regarding legitimate interests.

3. Transparency of the processing of personal data: data protection conditions

The processing of personal data must fully comply with the principles set out in Article 5 (1) of the CISA, including point (a). The principle of transparency presupposes that all information and messages related to the processing of personal data are easily accessible, comprehensible and clearly worded. In other words, data protection conditions must be in place. The content of the data protection conditions is regulated by Articles 12 - 14 of the CISA. The Supervision Authority reviewed the data protection conditions submitted by Penteer OÜ and pointed out the following deficiencies in the repeated proposal on 19.05.2021

Purpose and legal basis of the processing of personal data (Article 13 (1) (c) CCIP) 1.1.

The following are stated in the data protection conditions: The Client grants us the right to collect and process the Client's personal data if he wishes to rent sports equipment at his own discretion and with his consent. These are: first and last name, personal identification code, telephone number, contact address, e-mail address, copy of identity document. We explain that in a situation where the transmission of data for the use of equipment is mandatory, ie the service cannot be used without the transmission of data, there can be no data processing on the basis of consent within the meaning of the ICRM. Consent can only be used as a basis for the processing of personal data in cases where the processing of personal data (including collection) is not unavoidable and the person can really decide whether or not he or she wishes to give consent. Failure to give consent must not have negative consequences. In other words, in case of consent, it should be possible to use the service without transmitting data, Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235. In the present case, however, it is understood that the service cannot be used without the transfer of all personal data. Although entering into the agreement is voluntary, the transfer of data in a specific case is not based on consent, but because it is necessary for you to ensure the conclusion and performance of the agreement. Thus, the reference to consent must be removed from the data protection conditions and, in cases where the processing of data is necessary for the conclusion of a contract or the fulfillment of obligations under the contract, it must also be mentioned in the data protection conditions.

1.2.

Also, the collection of copies of identity documents does not comply with the requirements set out in Articles 5 and 6 of the CCP, therefore OÜ Penteer is prohibited from further collecting copies of identity documents from all customers

and the relevant information must be removed from the data protection conditions. In a situation where a person uses an installment payment service (eg LHV installment payment), it may be necessary to collect a copy of an identity document, but in this case it is necessary for the financial service provider (LHV) and not for OÜ Penteer. In such a case, OÜ Penteer could be the authorized processor of the financial service provider, who fulfills the obligation provided to the financial service provider and forwards the necessary data (incl. A copy of the identity document) to the financial service provider.

2. Period of retention of personal data or, if this is not possible, the criteria for determining such a period (Article 13 (2) (a) CISA) 2.1. In the data protection conditions you state the following: We retain the Client's personal data for as long as we deem it necessary for the fulfillment / achievement of purposes or as provided by law (eg accounting and tax laws, money laundering and terrorist financing prevention law, procedural laws governing deadlines) but not more than 7 years from the end of the Customer Relationship. We explain that the retention period for personal data must be worded in such a way that the person can assess the retention period for specific data / purposes based on their situation. In the present case, this remains incomprehensible. At the same time, the Supervision Authority does not understand in which cases the Money Laundering and Terrorist Financing Prevention Act applies to the processing of personal data of customers and which procedural laws you refer to in the data protection conditions. Therefore, if you have an obligation to retain data under the Money Laundering and Terrorist Financing Prevention Act and procedural laws, you must also indicate which data or in which case (for purposes) it is necessary to retain. Reference should also be made to specific procedural laws. We note that it is only possible to keep basic accounting documents for 7 years (see § 12 (1) of the Accounting Act). In addition, you are not in a position to regulate the retention of personal data for the purpose of protecting or submitting any legal claims. We further explain that the limitation period for a claim arising from a transaction is three years (§ 146 (1) of the General Part of the Civil Code Act) and in only individual cases the limitation period may be up to ten years (§ 146 (4) of the General Part of the Civil Code Act). Thus, in a situation where the data controller wishes to keep the data in general for longer than the normal limitation period (three years), this need must be very clearly justified. In the data protection conditions, you have stated that you will keep the data for a maximum of 7 years, but this is not enough and, as stated, the 7-year retention period is Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 is generally applicable only to the retention of source documents arising from the Accounting Act.

3. Information on the right to request the controller to access, rectify or delete personal data concerning the data subject or to restrict the processing of personal data or to object to the processing of such personal data, as well as

information on the right to transfer personal data (Article 13 (2) (b)) 3.1. The information set out in Article 13 (2) (b) of the CCIP is not included in the data protection conditions. We emphasize that all information provided for in Article 13 (1) and (2) of the CISA must be visible from the data protection conditions, including the right to request, rectify or delete personal data or to restrict the processing of personal data. The data protection conditions must also include information that a person has the right to request the transfer of personal data to another data processor and you are also obliged to transfer the data if it is technically feasible and does not infringe on the rights and freedoms of other persons. 4. Information on the right to lodge a complaint with the supervisory authority (Article 13 (2) (d) CCIP) 4.1. There is no information in the data protection conditions that a person has the right to submit a complaint to the supervisory authority (the Data Protection Inspectorate). 5. Information on whether the provision of personal data is a legal or contractual obligation or a requirement for the conclusion of the contract, as well as whether the data subject is obliged to provide such personal data and the possible consequences of not providing such data (Article 13 (2) (e)) 5.1. There is no information in the data protection conditions that the collection of data is a necessary requirement for the fulfillment of the obligations arising from the contract or the conclusion of the contract (see section 1.1 of the deficiencies in the data protection conditions). You also refer to the Money Laundering and Terrorist Financing Prevention Act and the procedural laws in the data protection conditions, but there is no information as to what data and in which cases you are obliged to process (incl. Collect and store) under the above laws. If the collection of data is a requirement arising from a contract or legislation, then the data protection conditions must also state that in a situation where the data is not transferred to you, you will not be able to provide the service. The representative of Penteer OÜ responded to the repeated proposal, according to which correct data protection conditions had to be prepared no later than 02.06.2021, as follows: In connection with finalize the data protection conditions and submit them to AKI and the Client's website. We explain that on 19.05.2021 the Inspectorate has made a proposal to Penteer OÜ to stop collecting copies of identity documents. This is due to the fact that, in the opinion of the Inspectorate, Penteer OÜ does not have a legal obligation to collect copies of identity documents and Penteer OÜ has not sufficiently proved the existence of a legal basis for the Inspectorate itself. The Inspectorate has also proposed on 28.04.2021 and 19.05.2021 to prepare and transmit to the Inspectorate data protection conditions that fully comply with the requirements set out in Articles 12 - 14 of the CISA. Therefore, Penteer OÜ must immediately bring its operations into compliance with the requirements set out in the IKÜM at 39 Tatari tn 39/10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee and prepare the correct data protection conditions. Even if Penteer OÜ does not agree

with the position of the Inspectorate regarding the collection of copies of identity documents, the data protection conditions must be prepared in this respect at its own discretion. In addition, we emphasize that the shortcomings in the data protection conditions do not only apply to copies of identity documents. Summary In view of the above, Penteer OÜ does not have a legal basis (the legal basis has not been sufficiently proven) to process (collect and store) copies of identity documents. In addition, the processing of personal data does not comply with the principles set out in Article 5 (1) (a) of the CISA - the processing is lawful; - the processing is transparent to the data subject. If the processing of personal data does not comply with the principles set out in Article 5 of the CISA, the processing of personal data is prohibited. Compliance with these principles is the responsibility of the controller himself (see Article 5 (2) of the CISA). Therefore, the collection of copies of identity documents must be stopped immediately. The correct data protection conditions must also be drawn up and published on the website. Pursuant to § 58 (1) of the Personal Data Protection Act and Article 58 (2) (d) and (f) of the General Data Protection Regulation, the Supervision Authority has the right to order the data controller to comply with the requirements of the CISA Restriction on the processing of personal data, including a prohibition on processing. Taking into account the factual circumstances and the fact that personal data are processed unlawfully in a particular case end the offense as soon as possible. / digitally signed / Raiko Kaur, lawyer, authorized by the Director General