

FOR PRIVACY PROTECTION AND STATE TRANSPARENCY Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee /
www.aki.ee Registration code 70004235 PRELIMINARY WARNING in personal data protection case no. 2.1.-4/22/916 Issuer
of the injunction Data Protection Inspectorate lawyer Ivo Eevel Time and place of issuing the injunction: 25.07.2022 in Tallinn
Addressee of the injunction/ personal data processor: Osta Pilet OÜ registry code 14304264 address: Pirita tee 26c/1-10,
12011 Tallinn e- mail address: as@bstars.eu Person in charge of the personal data processor: Board member RESOLUTION:
§ 56 (1), (2) point 8, § 58 (1) of the Personal Data Protection Act (IPS) and Article 58 (2) points d of the General Regulation on
Personal Data Protection (IKÜM) and on the basis of f, I issue a mandatory injunction for compliance: 1. bring the data
protection conditions into line with the conditions set forth in paragraphs 1-2 of Article 13 of the IKÜM (including taking into
account the explanations of the inspection); 2. remove third-party cookies from the website www.ostapilet.ee or obtain
voluntary consent from people to use such cookies; 3. send a confirmation to the inspectorate about the removal of cookies or
prove the voluntary consent of individuals to use cookies. I set the deadline for the execution of the order to be 15.08.2022.
Report compliance with the order to the Data Protection Inspectorate by this deadline at the latest. REFERENCE FOR
DISPUTES: This order can be challenged within 30 days by submitting either: - an appeal under the Administrative Procedure
Act to the Data Protection Inspectorate or - an appeal under the Code of Administrative Procedure to the Administrative Court
(in this case, the appeal in the same matter cannot be reviewed). Challenging a precept does not stop the obligation to fulfill it
or the implementation of measures necessary for fulfillment. PENALTIES WARNING: If the injunction has not been complied
with by the specified deadline, the Data Protection Inspectorate will impose a penalty of 5,000 euros on the recipient of the
injunction based on § 60 of the IKS: a penalty of 5,000 euros for each point of the injunction. 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 injunction in accordance with Article 58(2) of the Personal Data
Protection Act may result in a misdemeanor proceeding based on § 69 of the Personal Data Protection Act. For this act, a
natural person may be fined up to EUR 20,000,000, and a legal person may be fined up to EUR 20,000,000 or up to 4 percent
of its global annual turnover of the previous financial year, whichever is greater. The out-of-court procedure for a misdemeanor
is the Data Protection Inspectorate. FACTUAL FACTS: 1. During the self-initiated supervision procedure, the Data Protection
Inspectorate checked how Osta Pilet OÜ (hereinafter also the data processor) has complied with the IKÜM and it became clear

that Osta Pilet OÜ has not fulfilled the requirements arising from the IKÜM, because the data protection conditions can be found on the website www.ostapilet.ee did not comply with article 13 of the IKÜM. 2. The Data Protection Inspectorate made a proposal to Osta Pilet OÜ on 29.03.2022 to bring the data protection conditions found on the website ostapilet.ee into line with the conditions set out in paragraphs 1-2 of article 13 of the IKÜM (including taking into account the inspector's explanations) and asked to fulfill the proposal no later than 16.05. 2022 and send the corresponding confirmation to the Data Protection Inspectorate, and also recommended adding a cookie consent/refusal form to the website. 3. The inspection did not receive a response to the proposal by the specified date. Also, by the said date, the data protection conditions found on the website had not been harmonized and the consent/refusal form for the use of cookies had not been added, as a result of which the inspection made a re-introduction to Osta Pilet OÜ¹ on 30.05.2022 to bring the data protection conditions into line with the general regulation on the protection of personal data and to add the consent/refusal form for the use of cookies. AKI set 11.07.2022 as the deadline for completing the proposal. 4. By the deadline set by AKI, the inspectorate has not received a response from Osta Pilet OÜ, and the data protection conditions on the website ostapilet.ee have not been brought into line with IKÜM art. 13, and there is still no consent/refusal form for the use of cookies. 1 The e-mail was sent to the company's e-mail address as@bstars.eu indicated in the business register, as well as to the e-mail address indicated on the website www.ostapilet.ee and to the OSTAPILET klienditoe e-mail klienditugi@ostapilet.ee

FOUNDINGS OF THE DATA PROTECTION INSPECTION: 1. The most important shortcomings identified in the data protection conditions: The privacy conditions² found on the ostapilet.ee website do not meet the requirements set forth in the IKÜM, i.e. the data processor has not fulfilled the requirements arising from the regulation. The inspectorate analyzed the compliance of the privacy terms (hereinafter the Terms) found on the Ostapilet.ee website with Article 13 of the General Data Protection Regulation, i.e. whether the terms contain information that must be provided when receiving personal data if personal data has been collected from a data subject³. The inspection identified significant deficiencies in the conditions: 1.1. The purpose and legal basis of personal data processing (Article 13, paragraph 1, point c of the General Data Protection Regulation) There must be a legal basis and purpose for any processing of personal data (including collection and transmission to third parties). 1.1.1. Clauses 3.3 and 3.4 of the terms and conditions state the purposes and legal bases of the processing, but they do not match clause 10.7 of the terms of use⁴ (hereinafter the terms of use) found on the website, according to which personal data is processed only for the purposes of service provision (mediating the purchase of a ticket, distributing a newsletter, creating a payment option). Thus,

misleading information is provided to the person and it is contrary to the requirements of Article 12, paragraph 1 of IKÜM, i.e. it is not clearly clear to the data subject. 1.1.2. The purposes stated in the terms and conditions (except in clauses 3.4.4-3.4.6) for which personal data are processed remain incomprehensible to the inspection. For example, according to point 3.4.1, personal data is processed for security and safety purposes. The inspection does not understand what is meant by this. Nowhere does it appear that OÜ Osta Pilet is involved in providing security and safety in addition to the mediation of ticket sales. Therefore, if it is a mistaken purpose, a change in the terms should be made, if not, what is meant by it should be spelled out more clearly. The same applies to point 3.4.2. According to the conditions displayed on the website, an order is not made on the website, but a purchase is made, therefore the purpose of processing personal data for the purpose of processing the order remains incomprehensible to the inspection. Therefore, if it is a mistaken purpose, a change in the terms should be made, if not, what is meant by it should be spelled out more clearly. 2

<https://ostapilet.ee/est/information/users-1/privaatsuspoliitika-15> 3

<https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679# :~:text=13-,>

Information%2C%20what%20must%20be%20given%20when%20personaldata%20is%20collected%20from the data subject 4

https://ostapilet.ee/est/information/users-1/ostapilet_kasutustimidesum- 11 The processing of personal data to ensure the functioning of e-shop services, i.e. point 3.4.3, also remains incomprehensible to the inspection. If it is a wrong purpose, a change should be made in the terms and conditions, if not, then more clearly explain what is meant by it and analyze whether and which personal data need to be processed for this purpose. In addition, I would like to draw attention to the fact that personal data is transferred by the ticket seller to the organizer on the basis of article 6 paragraph 1 point b of IKÜM, i.e. on the basis that it is necessary for the performance of the contract, only those personal data that are necessary for the performance of the contract may be transmitted. In doing so, the principles of data processing stipulated in IKÜM must be followed. I would separately point out here the "restriction of gathering as little data as possible" provided for in Article 5(1)(c) and the "purpose limitation" provided for in Article 5(1)(b). If the tickets are not personalized, it is not possible to transmit the buyer's name, e-mail or address to the event organizer for the purpose of fulfilling the contract, because these data are not necessary for the event organizer to fulfill the contract. 1.2. If the legal basis for processing is a legitimate interest (Article 6(1)(f) of the GDPR), then information about the legitimate interests of the data controller or a third party (Article 13(1)(d) of the GDPR) , whether to add to the data protection conditions or add information on how it is possible to view the analysis (e.g. to view the legitimate

interest analysis, send an email to the e-mail address ostapilet@....). In this case, the legitimate interest analysis has not been included either on the website or in the privacy settings.

1.3. Information on recipients or categories of recipients of personal data (Article 13(1)(e) of the GDPR)

The term "recipient" is defined in Paragraph 9 of Article 4 of the GDPR as "a natural or legal person, public sector institution, office or other body to whom personal data is disclosed, regardless of whether it is a third party or not". Thus, the recipient does not have to be a third party. Therefore, the term "recipient" includes other controllers, co-processors and authorized processors to whom data is transferred or disclosed, and information about such recipients should be provided in addition to information about third-party recipients. The actual (named) recipients of personal data or categories of recipients must be provided. In accordance with the principle of fairness, controllers must provide information about recipients that is most relevant to data subjects. In practice, these are usually named recipients so that data subjects know exactly who has their personal data. If controllers decide to provide categories of recipients, the information should be as specific as possible, showing the type of recipient (i.e. indicating their fields of activity), industry, sector or sub-sector and the location of the recipients.

1.3.1. In p. 3.5 of the terms and conditions it is referred to "The data processor has the right to share the personal data of customers with third parties, such as authorized data processors, accountants, transport and courier companies, providers of transfer services

5 In doing so, the legitimate interest must be determined for the benefit of the data subject. See Article 29 working group guidelines on transparency under Regulation 2016/679 on page 36 and AKI's legitimate interest guide

6 Article 29 working group guidelines on transparency under Regulation 2016/679

companies. The data processor is the controller of personal data. The data processor transmits the personal data necessary for making payments to the authorized processor Maksekeskus AS.

1.4. The conditions do not clarify who the authorized persons of the data processor are (except Maksekeskus AS) or what personal data is transmitted to each recipient. In the same way, the need to share personal data with transport and courier companies remains incomprehensible (how the said companies are related to mediating ticket sales for cultural events). If there is a mistake, a change to the terms should be made.

1.4.1. In addition, I would like to point out that the mentioned point is not in accordance with point 10.5 of the terms of use, in which it is stated "By purchasing a Ticket or registering as a regular customer, the Buyer consents that OSTAPILET may process the Buyer's personal data. The consent also includes the right of the OSTAPILET to transfer the Buyer's personal data to companies belonging to the same group as him, and in the event of a change of ownership of the OSTAPILET to the acquirer of the OSTAPILET. Personal data will not be forwarded to other persons. "Thus, the person is given misleading

information and it contradicts the requirements stated in Article 12(1) of the IKÜM, i.e. it is not clearly clear to the data subject.

1.5. The period of data storage or the criteria for determining the period of time (Article 13(2)(a) of IKÜM) The storage period is related to the requirement to collect as little data as possible in Article 5(1)(c) of IKÜM and the requirement to limit storage in Article 5(1)(e) of IKÜM. The retention period (or the criteria for determining it) may be dictated by factors such as statutory requirements or industry guidelines, but should be worded in such a way that the data subject can assess, based on their own circumstances, what the retention period is for specific data/purposes. It is not enough if the data controller states in general terms that personal data will be stored for as long as necessary to achieve the legitimate purposes of the processing. Where appropriate, different retention periods should be provided for different types of personal data and/or different purposes of processing, including, if necessary, the period of archiving⁷. Clause 3.4 of the terms and conditions. the subsections state how long personal data processed for a particular purpose will be stored. Sections 3.4.1 and 3.4.5 provide that personal data is stored at most according to the deadlines specified in the law. Therefore, the deadline specified in points 3.4.1 and 3.4.5 does not meet the requirements of article 13, paragraph 2, point a of IKÜM.

1.6. Information on the right to request from the data controller access to personal data concerning the data subject and their correction or deletion or restriction of personal data processing or to object to the processing of such personal data Clause 2 point b) Clause 4 of the terms and conditions states the rights of the data subject. According to this, the data subject has the right to: get access to his personal data and get acquainted with them (4.1), get information about the processing of his personal data (4.2), supplement or correct inaccurate data (4.3). This directly contradicts IKYM art 13 paragraph 2 point b. Namely, IKÜM art. 13 paragraph 2 provides what information the controller must provide to the data subject when receiving personal data, and according to IKÜM art. 13 paragraph 2 point b, this is information about the right to request from the controller access to personal data concerning the data subject and their correction or deletion or restriction of personal data processing, or to object to the processing of such personal data, as well as information on the right to transfer personal data. The guidelines of the Article 29 working group on transparency according to Regulation 2016/6798 emphasize that, in particular, the data subject's right to object to the processing of personal data should be explicitly drawn to the data subject's attention at the time of the first notification at the latest, and this must be presented clearly and separately from any other information. IKÜM Article 18 sets out the grounds on which a person has the right to demand from the data controller to limit the processing of personal data, i.e. to mark stored personal data with the aim of restricting their further processing, and according to IKÜM Article 21, a person has the right,

based on his specific situation, to object at any time to the processing of personal data concerning him, which takes place on the basis of Article 6(1)(e) or (f), including profiling based on these provisions. The inspection emphasizes that all the information stipulated in paragraphs 1 and 2 of Article 13 of the IKÜM must be visible from the data protection conditions. The contradiction also occurs in Clause 3.1 of the Terms and Conditions and Clause 10.4 of the Terms of Use. between, according to which OSTAPILET collects and processes the following personal data of the Buyer: first and last name, e-mail address and telephone number, and the name of the regular customer, which enable the Buyer to be identified and which the Buyer has provided on the website when buying a Ticket or registering as a regular customer. This does not show that the data processor also processes payment card details⁹. Thus, misleading information is provided to the person and it is contrary to the requirements of Article 12, paragraph 1 of IKÜM, i.e. it is not clearly clear to the data subject. It also remains unclear to the inspection what data and for what reason the data processor collects about the client from public registers¹⁰. I point out that the data processor must follow the principle of minimality when collecting personal data, i.e. data must be collected as little as possible to achieve a certain goal. Just in case, data collection is illegal. Therefore, if you do not actually collect data from public records, a change to the terms should be made.

⁸https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_maaruse_2016679_kohase_labipaistvuse_kohta.pdf ⁹ Clause 3.1.4. ¹⁰ Clause 3.2 of the terms and conditions

2. Cookies used on the website

The Data Protection Inspectorate drew the data processor's attention to the fact that Osta Pilet OÜ uses cookies on the consumer's end device on its website www.ostapilet.ee without asking the person for their consent. I explain that in a situation where Osta Pilet OÜ installs third-party cookies on its website, Osta Pilet OÜ is the responsible processor in this regard, and there must be a specific legal basis for installing cookies. 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 equipment and access to information already stored therein is permitted only on the condition that the subscriber or user concerned has given their consent. , and has been provided with clear and understandable 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-673/171. 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. In this case, data is collected about the user without asking the consent of the data subject, which means that the data subject cannot decide on the use of cookies. 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 website www.ostapilet.ee is illegal in this case. This type of processing is permitted if the consent of the person in accordance with Article 7 of IKÜM is obtained for the use of cookies. 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. Therefore, a person must be able to give his consent for the cookies (for example, by actively ticking the boxes) that he allows to be used. If consent is not given, the use of third-party cookies is prohibited.

3. Summary According to IKS § 58 paragraph 1 and IKÜM article 58 paragraph 2 points d and f, the inspectorate has the right to order that the data processor bring personal data processing operations into compliance with the provisions of IKÜM in a certain way and within a certain period of time, the right to establish a temporary or permanent limitation of personal data processing , including the prohibition of processing. Taking into account the factual circumstances, including the fact that Osta Pilet OÜ has not proven to the inspection the fulfillment of the IKÜM requirements (Articles 5, 6, 12 and 13) and the website www.ostapilet.ee has several important deficiencies, the inspection finds that the mandatory issuing an injunction in this matter is necessary to end the offense as soon as possible. (digitally signed) Ivo Eevel lawyer under the authority of the Director General