



National number: 0611-394/2021

IMI Case Register entry: 512935

Date: 9. 2. 2024

The Information Commissioner (hereinafter referred to as: IP) hereby issues, under the State Supervisor for Personal Data Protection [REDACTED], on the basis of Articles 2 and 8 of the Information Commissioner Act (Official Journal of the Republic of Slovenia, No. 113/2005, with amendments and additions; hereinafter referred to as: ZInfP), Articles 36, 37 and 119(1) of the Personal Data Protection Act (Official Journal of the Republic of Slovenia, No. 163/22; hereinafter referred to as: ZVOP-2), Article 135(4) of the General Administrative Procedure Act (Official Journal of the Republic of Slovenia, No. 24/06 — UPB2, 126/07, 65/08, 8/10, 82/13, 175/20 — ZIUOPDVE and 3/22 — Zdeb; hereinafter referred to as: ZUP) in conjunction with Article 3(2) of the Inspection Act (Official Journal of the Republic of Slovenia, No. 43/07 — UPB1 and 40/14; hereinafter referred to as: ZIN) and Article 56(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter referred to as: GDPR), in the matter of carrying out inspection of the implementation of the provisions of the GDPR and the ZVOP-2 at [REDACTED] (hereinafter: the controller), ex officio the following

### DRAFT DECISION

1. The inspection procedure conducted by the IP at the controller [REDACTED], under national No. [REDACTED], in which the controller voluntarily rectified all illegalities, irregularities and deficiencies found during the procedure, is closed.
2. No specific costs have been incurred by the authority and the controller bears his own costs of the proceedings.

### Findings and reasoning

The inspection procedure was conducted by the IP, on the basis of the received complaint, filed by the Hungarian individual ([REDACTED]) at the Hungarian Competition Authority and then transferred to the Hungarian Data Protection Authority (hereinafter referred to as: Hungarian DPA). The complaint in question gave rise to allegedly inadequate security of the payment card data and a request for deletion of the data of the complainant, which were indicated by the complainant when entering the data on the purchase of the item on the website [REDACTED].

On 6 July 2021, the Hungarian DPA launched, via the Internal Market Information System (hereinafter: IMI), under the cooperation mechanism provided for in the GDPR, the procedure for the identification of a lead supervisory authority in accordance with Article 56 of the GDPR. It was established that the sole place of establishment of the controller is in [REDACTED] and that the processing significantly affects or could significantly affect individuals in more than one Member State, since the controller, in addition to the online store at [REDACTED], also manages online shops at [REDACTED], [REDACTED], [REDACTED] and [REDACTED]. Therefore, IP confirmed, through IMI system, on 19 July 2021, that it will conduct the procedure as the lead supervisory authority (hereinafter referred to as: LSA).

Within the framework of the cooperation mechanism, the IP forwarded preliminary draft decision on the 5 June 2023 to the concerned supervisory authorities for an opinion (according to procedure A61VMN 513203), in connection with which the Hungarian supervisory authority forwarded comments. Taking into account the comments of the Hungarian supervisory authority, the IP issued a draft decision on 29 December 2023 (according to procedure A60 DD 591435) and forwarded it to the relevant authorities for their opinion, but did not receive any comments to it.

The investigation conducted by the IP concerned two issues, namely (1) whether the controller complied with the request of the complainant for deletion of his personal data; and (2) whether controller ensured appropriate level of security of personal data processed in relation to payment cards.

According to the information indicated in the complaint, the IP firstly investigated the controller's website (doc. No 0611-394/2021/4 of 13.10.2021) and asked him to provide written explanations, documentation and statements (doc. 0611-394/2021/5 of 30.11.2021). In its request, the IP briefly explained to the controller the procedure for cooperation between supervisory authorities in accordance with the procedure laid down in Article 60 of the GDPR.

Regarding the complainant's data in the present case, the controller on 21 December 2021 (doc. No 0611-394/2021/6) explained that personal data relating to him are no longer stored. If it were stored and the data was entered from an unfinished purchase process, it would not be a systemic error, but rather a result of functionality embedded in the website (so-called "abandoned cart" functionality).

On 22 November 2022 the IP requested the controller to provide additional explanations, documentation and statements (doc. No 0611-394/2021/7), to which the controller replied on 7 December 2022 (doc. No 0611-394/2021/8). In its reply, the controller provided a more general description of the procedure for the erasure of personal data at the request of an individual.

Additionally, on 13 April 2023 the IP requested the controller (via its DPO) to provide a contract between the controller and the company ██████, which provides online payment card processing for the controller (doc. No 0611-394/2021/9). The controller sent the requested contract to the IP the same day (doc. No 0611-394/2021/10).

Based on the explanations and documentation provided by the controller, the IP summarises the key findings of the investigation procedure:

#### **I. Regarding a request for the erasure of all personal data processed by the controller in relation to the complainant**

*Article 17 of the GDPR provides that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*

*(a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;*

*(b) the data subject withdraws consent on the basis of which the processing takes place pursuant to point (a) of Article 6 (1) or point (a) of Article 9 (2), and where there is no other legal basis for the processing;*

*(c) the data subject objects to the processing pursuant to Article 21 (1), and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21 (2);*

*(d) the personal data have been unlawfully processed;*

*(e) the personal data must be erased in order to comply with a legal obligation pursuant to Union or Member State law to which the controller is subject;*

*(f) the personal data have been collected in connection with the provision of information society services referred to in Article 8 (1).*

It is apparent from the documentation obtained that the complainant [REDACTED] received on 11 October 2020 a message from the e-mail address [REDACTED] about the placed order ([REDACTED]) with a summary of the order placed on the type of goods ordered, discount, final price, VAT, handling costs, delivery address, billing address, delivery method and method of payment.

The complainant [REDACTED] replied on the same day (11 October 2020) to the e-mail address [REDACTED], that he did not place the order [REDACTED], but only browsed the controller's website and therefore requested the deletion of the order and all personal data relating to him as well.

The controller also replied on the same day (11 October 2020), from the e-mail address [REDACTED], that there was most likely a systemic error and that his order had been cancelled and the data deleted.

On 13 October 2020 the complainant received an advertisement from [REDACTED] and then again on 15 October 2020. Therefore, the complainant sent another request for the deletion of all his data from the controller's system (on 15 October 2020), to the e-mail address [REDACTED] and received a reply that his e-mail address had been deleted from the messaging (marketing) system. After that date, the complainant did not receive any advertising messages from the controller anymore.

In its reply of 11 February 2021 to the Hungarian DPA, the controller confirmed, that the complainant [REDACTED] had indeed requested the deletion of the order and any personal data relating to him on 11 October 2020, by e-mail [REDACTED]. The controller immediately complied with his request and replied on the same day that he had deleted his data. He admitted that the complainant had indeed received an e-mail of a commercial nature. Consequently, on 15 October 2020 the controller deleted his e-mail address also from the list of e-mail addresses and informed the individual thereof on the same day. He added that there was probably a systemic error in the conclusion of the order, since the system recorded the order as concluded, even though the individual [REDACTED] did not click on the 'Submit order' button. However, the controller also allowed the possibility for the complainant to actually concluded the order by himself. On the fact that no data relating to the order placed by a complainant or data relating to him, are no longer present in the controller's system, the controller submitted screenshots of its databases.

On 21 December 2021, the controller, upon the request of the IP (doc. No 0611-394/2021/5 of 30.11.2021), again confirmed, that he does not retain any data concerning the complainant [REDACTED], with e-mail address [REDACTED].

Upon the request of the IP (doc. No 0611-394/2021/7) the controller on 7 December 2022 provided a more general description of the procedure for the erasure of personal data at the request of an individual. The controller explained that individuals rarely submit such a request, however, where appropriate, the controller complies with it. The controller further explained, that its contractor [REDACTED], which provides hosting and operation of the online store and operation of the cash register, provides the functionality of deleting all data about a particular user by clicking ("Erase personal data"), about which the controller has also attached a screen image. The controller then informs the other processors of the deletion by e-mail.

## **II. Concerning the suspicion of inadequate protection of personal data relating to the processing of personal data by payment cards**

The complainant stated that personal data related to the payment card are processed directly on the website [REDACTED] and not via the secure platform to which the individuals are supposed to be redirected at the stage of entering payment card data. With regard to his allegation, the complainant did not provide any evidence.

The controller explained that the data related to the online payments are not processed on the website [REDACTED], but is carried out through the [REDACTED] system which ensures adequate security of personal data. Attached agreement (“[REDACTED]”) indicated that the agreement was concluded on [REDACTED] with [REDACTED].

On 17 December 2021, upon the request of the IP, the controller added, that in relation to the payments processing it has a signed agreement with its external partners [REDACTED] and [REDACTED] in order to ensure the processing of online payments by payment cards. The Agreement ([REDACTED]) has been attached by the controller to its explanations. However, as the agreement was allegedly extracted from the [REDACTED] system, there was no indication of the date that the agreement had been concluded on. Therefore, the IP requested additional evidence that would support the allegation of the controller with regard to the online payments system.

On December 8 2023 the controller provided additional explanations regarding the validity of the [REDACTED] Service Agreement. In this regard the controller explained that the [REDACTED] service has been used since 20 January 2021 (in this regard the controller enclosed the printout of all payments from the [REDACTED] system). However, the contract with [REDACTED] and [REDACTED] had been terminated lately on 14 October 2021 and as evidence the controller attached a document “Notice to terminate the [REDACTED] Agreement”.

According to the findings, in relation to the secure payments processing, at the time of the alleged purchase by [REDACTED] on 11 October 2020, the controller used the services of [REDACTED], and [REDACTED], and no evidence was found in the inspection procedure that would make it possible to impose responsibility to the controller of inadequate security of personal data related to the payment cards and, therefore, of an infringement of Article 32 of the GDPR.

To conclude, in a view of the above-mentioned measures of the controller, by which it has rectified the non-compliances revealed ex officio within the investigation procedure and specifically, non-compliance with Article 17 of the GDPR, deleting the requested data of the complainant [REDACTED], thereby established a legitimate processing of personal data, IP concludes that, in the present case, it would be appropriate to continue the inspection procedure only if the inspection measure was necessary to order the correction of deficiencies and irregularities in relation to the processing of personal data or to order the prohibition of unlawful processing of personal data and to establish a legitimate processing for the future. In the specific case, all irregularities found in the course of the investigation procedure were rectified, therefore, in accordance with the fourth paragraph of Article 135 of the ZUP, in conjunction with the second paragraph of Article 3 of the ZIN and Article 2 of the ZInfP and Articles 57 and 58 of the GDPR should be closed, as is apparent from point 1 of the operative part of this Decision.

Under the third paragraph of Article 118 of the ZUP, the costs of the proceedings are to be decided in the decision terminating the proceedings. In the present proceedings, no special costs have been incurred, as is apparent from point 2 of the operative part of this Decision.

This Decision is issued ex officio and on the basis of Article 22 of the Administrative Fees Act (Official Journal of the Republic of Slovenia No. 106/10 — official consolidated text, 14/15 — ZUUJFO, 84/15 — ZZelP-J and 32/16) the fees are free.

**Instruction on Remedies:** There is no appeal against this decision, but an administrative dispute is allowed. The administrative dispute is initiated by an action, which is filed within 30 days of service of the decision at the Administrative Court of the Republic of Slovenia, Fajfarjeva 33, 1000 Ljubljana. The application is sent by registered mail to that court. The action, accompanied by any annexes, shall be filed at least in triplicate. The application must also be accompanied by this order in original or transcript.

[REDACTED]

State Supervisor for Personal Data Protection

Recipient:

- [REDACTED]