REPUBLIC OF SLOVENIA
INFORMATION COMMISSIONER
Dunajska cesta 22, 1000 Ljubljana
T: 01 230 9730
www.ip-rs.si
gp.ip@ip-rs.si

National number: 06110-413/2022
IMI Case Register entry: 469543
Date: 8. 3. 2023

The Information Commissioner (hereinafter: IP) 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: ZInfP), Articles 36 and 37 of the Personal Data Protection Act (Official Journal of the Republic of Slovenia, No. 163/22; hereinafter: ZVOP-2), Articles 57 and 58 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: GDPR), 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: 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: ZIN), in the matter of carrying out inspections of the implementation of the provisions of the GDPR and the ZVOP-2 at [redacted] (hereinafter: the controller), ex officio the following

DECISION

1. The inspection procedure conducted by the IP against the controller under No. 06110-413/2022 is terminated.
2. No specific costs were incurred in this procedure.

Findings and reasoning

The IP initiated the inspection procedure against the controller ex officio on the basis of a notification of a personal data breach (hereinafter: DBN), which has been sent to IP by the controller on 11 September 2022 in accordance with the provisions of Article 33 of the GDPR. The suspicion of inadequate insurance arose from the statements of the operator in DBN. The controller states that on 9 September 2022 he found that there had been a hacking (including [redacted] ransomware) attack on the controller's information system, that the extent and consequences of the attack were still being determined, as the analysis of the security incident had not yet been completed.

The inspection procedure was initiated on the basis of the Personal Data Protection Act (Official Gazette of the RS, no. 94/07-UPB1 and 177/20, hereinafter ZVOP-1), and in the meantime ZVOP-2 was adopted, which in the Article 119(1) stipulates that inspection procedures initiated on the basis of ZVOP-1 shall continue in accordance with ZVOP-2.

The controller provided very little information in the DBN. The State Supervisor for Personal Data Protection conducting the inspection procedure in question (hereinafter: the Supervisor), aiming to obtain more information about the controller, his services, the scope of business, the processing of personal data, and in order to be able to assess what obligations the IP as a Supervisory Authority has as a result of the DBN received in cross-border cooperation procedures under the GDPR, had carried out a review of the controller's website [redacted] on 13 September 2022.

Due to the need to clarify the case and establish the facts, on 15 September 2022 the IP requested the controller (hereinafter: request of the IP) to provide a written explanation, documentation and statement regarding the provision of information security in general and the security of personal data at the controller and regarding the handling of the security incident in question.

On 23 September 2022 the IP received a request from the controller for an extension of the deadline for reply, in which he explained that he was still intensively remedying the consequences of the hacking attack which partially paralyzed the controller's business and that his primary focus in this situation was to provide basic services to subscribers. The Supervisor complied with the controller's request and extended the deadline for replying to 17 October 2022.

IP received the response of the controller on the 17 October 2022. The controller replied to all the questions and attached the documents to which he referred in his answers. After examining the replies of the controller and the accompanying documentation, the Supervisor concluded that the controller had still not provided sufficient information and evidence to assess the appropriateness of the measures for the protection of personal data and the obligations of the IP as the lead supervisory authority in the cooperation procedure under the GDPR. In order to obtain all the necessary information and explanations, the Supervisor decided to hold a meeting with the controller, which was held on 8 November 2022.

Affiliated companies in the [redacted] are listed in Article 1 of the Personal Data Protection Regulations, which the controller provided in response to the IP request. In addition to the controller, the [redacted] also consists of:

- [redacted] Croatia,
- [redacted] Germany,
- [redacted], Italy,
- [redacted], Serbia,
- [redacted], Bosnia and Hercegovina,
- [redacted] Macedonia.

Currently, about [redacted] individuals are employed in all affiliated companies, of which [redacted] are employed at the controller. In companies outside Slovenia only affiliations in Croatia and Serbia have employees, the remaining companies are without employees. The affiliated companies have a common human resources management system (hereinafter: the HR system). The controller and the affiliated company in Croatia also use a common system for recording working hours [redacted] In the HR system, in addition to the data of the employees of the controller, only the personal data of individuals employed in affiliated companies are recorded. To manage employee data in accordance with the requirements of labour law, each related company uses its own solutions adapted to the requirements of national law. Affiliated companies, which have employees, also independently take care of the purchase and maintenance of the computer equipment used by the employees. All other processing of personal data, where the controller acts as a controller or processor of personal data of his customers, is centralised.

All affiliated companies use a common process management system (hereinafter: [redacted]), that is, accounting and invoicing for the services of the controller is centralised. This system was attacked. The clients of the controller are only legal persons, but in the [redacted] system there are also contact details of employees (individuals) for the purpose of communicating with customers. All affiliated companies also use a common customer relationship management system (hereinafter: CRM system). The CRM system is a web solution that has not been attacked.

The services of the controller are also centralised. Servers, which are also accessed by clients and processors, are hosted by [redacted] (only the rental of secure premises). The customer's services are based on vehicle location data, other vehicle data (temperature, fuel level, door, etc.) and on tachograph data from drivers (traffic routes, vehicle,.ddd files). Customers do not see the driver's data until they have entered a request for an inspection (the driver's name and surname). The data is stored on the driver card (.ddd files) and is readable by special programs.

Users log in to the controller's network with a username and password. The controller uses the [redacted] login to the system. There are [redacted] with administrative rights, and these [redacted] have shared rights and do not use [redacted] computers. Around [redacted] users access the system remotely, using only computers owned and maintained by the controller.

The controller has conducted an internal investigation of the security incident and informed the parties that employ (or are in a contractual relationship with) the individuals whose personal data was compromised during the attack about the findings and the measures taken. The contact information of these individuals is available

only to the customers of the controller. Employees of the controller and affiliated companies were informed by the controller himself. Information on the security incident for affiliated companies, which was also submitted to the IP, was prepared by the controller in English.

The results of the internal investigation confirmed that the following servers of the controller's IT system (Office segment) were affected by the attack:

- [redacted]

Two servers were affected in the service part (Production segment), namely:

- [redacted], e.g., from driver to dispatcher or from dispatcher to dispatcher). No data on recipients and senders were stored on this server or pseudonymised. The data that would allow de-pseudonymisation was located on a server that was switched off on time and the attackers had no access to it.
- [redacted] (contains temporary storage of application files, e.g., scanned accounts, CRM, photographs sent by drivers to dispatchers).

The controller did not agree to the demands of the attackers, but immediately after the attack was detected, he took a series of measures to protect the attacked system. The entire infrastructure and servers (whether attacked — encrypted or not) were turned off, formatted and reinstalled.

No data in the service part of the IT system was lost, so the controller was able to provide services to its customers within a few hours, while the other parts of the IT system were gradually restored.

As explained by the controller in response to the IP request, in order to prevent the possibility of re-intrusion to the same attackers, he also re-established the entire network, so that the attackers no longer have any advantage they would otherwise derive from their knowledge of the controller's IT architecture. He also carried out a series of additional measures to improve information security, about which, together with other information about the attack, he informed his partners.

Increased information security was also an explicit requirement prior to the transfer of ownership of the company. New owners [redacted] are also planning an external IT audit of the company's work and regular (including unannounced) penetration tests.

In the inspection process, it was not established which vulnerability the attacker has used to infiltrate the system. As the controller explained in his response to the IP request, the it considers that the intrusion started with the entry into the [redacted] server, as it found the first [redacted] installed on that server (according to the date of creation). Whether the attacker has taken advantage of any of the "zero-day" vulnerabilities of the [redacted] or has provided access to the system via a phishing message, is unlikely to be established as the attacker has deleted all traces.

The controller informed the IP, the Slovenian Computer Emergency Response Team (SI-CERT) and the Police about the attack. SI-CERT provided information which merely confirmed the conclusions reached by the controller himself and acted accordingly. On the 21 September 2022, the controller received a reply from the Police that a criminal investigation is being conducted

In the context of the analysis of the security incident, the controller did not detect increased traffic on the network or on the main switch of the network. Although at this moment, there are no indications that personal data has been disclosed or otherwise provided to third parties, the controller checks on a daily basis whether the personal data to which the attacker had access is published on the internet (including on the dark web) and has not detected the posts until now.

After examining the explanations provided by the controller and the documentation submitted, the IP found that, despite the fact that the breach in question did not pose a significant risk to the rights and freedoms of individuals whose personal data were compromised at the time of the attack, the controller had informed all affected individuals or partners who have contact details of those individuals of the consequences of the cyberattack, in accordance with the provisions of Article 34 of the GDPR, that the controller took appropriate measures to prevent such breaches in the future and to ensure the security of processing of personal data is in accordance with the provisions of Article 32 of the GDPR.

Since, in accordance with Article 4(23) of the GDPR, cross-border processing of personal data took place in the EU in the context of the activities of the sole establishment of the controller where the processing significantly affects or is likely to significantly affect data subjects in more than one Member State, the IP conducted the procedure in accordance with the rules on cross-border cooperation and compliance, as regulated by Sections 1 and 2 of Chapter VII of the General Regulation (in particular Articles 56 and 60 of the GDPR). On 27 December 2022, within the framework of the mutual assistance procedure (61VMN 469549), the IP informed the Supervisory Authority of Croatia as the concerned supervisory authority with the findings of the inspection procedure and the draft decision. Article 60 Draft Decision procedure (A60DD 484323) was launched on 7 February 2023. However, no relevant and reasoned objections were raised.

Since the suspicion of inadequate protection of personal data was not confirmed in the framework of the inspection procedure, the IP terminated the present procedure on the basis of Article 135(4) of the ZUP in conjunction with Articles 36 and 37 of the ZVOP-2 and Article 3(2) of the ZIN, as stated in 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].