UOOU-01752/21

Control of compliance with the obligations stipulated by the GDPR regulation in connection with a cyber attack on servers containing personal data, in relation to which the controlled person was in the position of administrator.

The review was initiated in November 2021 with an oral hearing and an on-site investigation at the auditee's headquarters based on a complaint received containing a suspected personal data breach in connection with a security incident related to a hacker attack undertaken on March 14, 2021 and based on a breach notification received security of personal data, according to which the aim of the attack was to encrypt data with the subsequent recovery of a financial sum.

The Office conducted an investigation of the facts related to the attack in question, including oral negotiations and local investigations at the controlled person and his processor, the company operating the servers affected by the hacker attack.

The inspectors found a violation of the provisions of Article 33, Paragraph 1 of the GDPR Regulation by not reporting this violation to the Office without undue delay and, if possible, within 72 hours of the moment when she became aware of the breach of personal data security. The inspected person provably became aware of the security breach on March 15, 2021 (by phone) and March 18, 2021 (in writing), while it was proven that he did not report the security breach until November 23, 2021.

According to the auditors, the audited person did not demonstrate compliance with the obligation set forth in Article 34, Paragraph 1 of the GDPR regulation, i.e. did not demonstrate that he would have notified data subjects of a breach of personal data security in an appropriate manner.

Furthermore, it was established that the controlled person violated the provisions of Article 33, Paragraph 5 of the GDPR regulation, because the personal data security violation documentation maintained by him does not contain the effects of the violation.

The audited person filed objections against the audit findings, while only the objection directed against the audit findings was (partially) accepted, in which it is stated that there was a violation of personal data protection security due to insufficient personal data protection settings by the processor. NÚKIB's statement showed that the installation of the server software patch from March 2, 2021 will not solve situations where the server is already compromised. According to NÚKIB's statement, the vulnerabilities could have been used as early as January 2021, while the hacker attack took place on March 14, 2021. Even from the documents provided by the inspected person and the processor, the Office was unable to find out when the

unauthorized access to the processor's servers occurred (because the date of the attack breach of personal data security may not match), and therefore whether the processor responded to the threat late. However, the Office added that even in the event of a cyber attack, the administrator is obliged to fulfill the obligations arising from the GDPR regulation and to document their fulfillment in accordance with Article 5, paragraph 2 of the aforementioned regulation.

The review was completed in December 2022 and the file was forwarded for the initiation of administrative proceedings.