Inspection of the operator of a non-state medical facility

The inspection was initiated on the basis of the notification of a case of breach of personal data security and, above all, on the basis of other facts discovered by the Office for Personal Data Protection as part of the actions preceding the inspection. As part of these actions, deficiencies in the security of the website were identified, which were not described in the initial notification of a breach of personal data security.

The subject of the inspection was compliance with the obligations set for the inspected person by Regulation (EU) 2016/679 and Act No. 110/2019 Coll., on the processing of personal data, in connection with the processing of personal data through electronic means of communication and their security in terms of personal data protection. Specifically, the inspection focused on possible violations of Article 24 and Article 32 of Regulation (EU) 2016/679 in the transmission of health examination results via websites.

The inspected person is the operator of a non-state medical facility that provides patients with a range of diagnostic examinations. On its website, it subsequently transmits the results of the examination, both to patients and to the doctors who recommended the examination. This results in the processing of health data, i.e. special categories of personal data in the sense of Article 9, paragraph 1 of Regulation (EU) 2016/679. The subject of the security breach notification was an attack on the website by an unknown attacker (later identified by the Police of the Czech Republic), who then sent an e-mail message to the inspected person to draw attention to the shortcomings regarding the password used to access the examination results, and to the weak security of the protocol of the site itself. Following this event, the audited person stopped the operation of the website in question and proposed technical measures for higher security. However, the Office found that other websites operated by the inspected person for the purpose of transmitting examination results show the same deficiencies. However, their operation was not restricted and no new technical measures were implemented.

The inspection carried out revealed a violation of the personal data controller's obligations arising from Article 24 and Article 32 of Regulation (EU) 2016/679, as the controlled person did not take such technical and organizational measures to ensure and be able to document that the processing of personal data is carried out in accordance with Regulation (EU) 2016/679, or did not implement such technical and organizational measures to achieve a level of security corresponding to the given risk. The

inspected person used an unsecured communication protocol and a weakly secured access password for websites making examination results available. In addition, the same password for making the results of the examination available was given to both the data subject and the doctor who requested the examination. There was no record keeping of accesses to personal data, and administrative access to the system for making the examination results available, which the processor of personal data has, was not registered and was secured only by a password with a strength of three characters. The controlled person thus lacked the ability to ensure the continuous confidentiality of personal data contained in the examination results. The inspected person began to correct the problematic situation already at the time of the ongoing inspection, when he introduced a secure protocol on the website, changed the system for creating access passwords and implemented measures to prevent random attempts to gain unauthorized access to the examination results, in the form of blocking the IP address in case of repeated entry wrong password.

However, the remedial measures taken were only partial and were not implemented on all websites making the examination results available, therefore the Office will impose remedial measures as part of subsequent administrative proceedings.

Additional information:

Adequate and constant attention must be paid to the security of the processing of special categories of personal data, taking into account the riskiness and sensitivity of the processing of such data. All measures increasing the security of processing must be implemented on the relevant information system as a whole and these measures must be regularly revised.