16.03.2023

Sanctions for GDPR violations

In February 2023, the National Supervisory Authority completed two investigations of operators in the medical field.

The investigations were started as a result of notifications received from individuals who complained about a possible violation of Regulation (EU) 2016/679.

As such, it was found that:

The operator of Dr. Furtună Dan Medical Center violated the provisions of art. Art. 32 para. (1) lit. b) and art. 32 para. (2) of Regulation (EU) 2016/679 and was fined in the amount of 4,918.50 RON (the equivalent of 1000 EURO).

The operator Med Life S.A. violated the provisions of art. Art. 32 para. (1) lit. b) and art. 32 para. (2) and para. (4) of Regulation (EU) 2016/679 and was fined 14,755.50 lei (the equivalent of 3000 EURO).

1. During the investigation, the National Supervisory Authority found that the operator of the Dr. Furtună Dan Medical Center sent a message to the phone number of a natural person, via the WhatsApp application, containing the results of two medical tests that belonged to two other people targeted.

From the checks carried out, it emerged that the operator of the Dr. Furtună Dan Medical Center did not implement adequate technical and organizational measures in order to ensure a level of security corresponding to the processing risk, including the ability to ensure confidentiality, integrity, availability and continuous resistance of systems and services Processing.

Consequently, this breach led to the violation of the confidentiality of processed data through the unauthorized disclosure and unauthorized access to certain personal data (such as: name and surname, CNP, telephone number, medical test result) transmitted through the WhatsApp application.

At the same time, the operator was also given the corrective measure to review and update the technical and organizational measures implemented as a result of the risk assessment for the rights and freedoms of individuals, including the work procedures related to the protection of personal data. At the same time, it was decided that the operator should implement a register relating to all cases of personal data security breaches, which would include a description of the factual situation regarding the personal data security breach, its effects and specifying the remedial measures taken , according to art. 33 para. (5) of Regulation (EU) 2016/679.

2. During the investigation carried out at the operator Med Life S.A., following a notification, it was found that a patient

received, by e-mail, in addition to his own investigation bulletin, a series of attached files containing the results of investigations belonging to five other patients. The attached documents contained the name, surname, date of birth, date of examination, reason for the examination, result of the investigation (examination), diagnosis, conclusions resulting from the medical examination.

As such, it turned out that the operator Med Life S.A. has not implemented adequate technical and organizational measures in order to ensure a level of security corresponding to the risk presented by the processing, generated in particular, accidentally or illegally, by the unauthorized disclosure of personal data stored or processed in another way, including the ability to ensure their confidentiality.

It was also found that Med Life SA did not take measures to ensure that any natural person who acts under the authority of the operator and who has access to personal data only processes them at the request of the operator.

Pursuant to art. 58 para. (2) lit. d) from Regulation (EU) 2016/679, the operator was ordered and the corrective measure to review and update the technical and organizational measures implemented as a result of the risk assessment for the rights and freedoms of individuals, including the work procedures related to the protection of personal data personal, as well as the implementation of a procedure for notification of personal data security breaches.

Legal and Communication Department

A.N.S.P.D.C.P