04/03/2023

Penalty for GDPR violation

In March 2023, the National Supervisory Authority completed an investigation at the operator Banca Transilvania SA and found a violation of the provisions of art. 5 para. (1) lit. a) and para. (2), art. 12 and art. 13, in conjunction with art. 83 para. (5) lit. a) and b) of Regulation (EU) 2016/679.

As such, the operator was fined 9,841.80 lei (equivalent to 2,000 EURO).

The investigation was started as a result of a complaint submitted by a natural person who reported a possible violation of the provisions of Regulation (EU) 2016/679.

Thus, the petitioner (client) requested Banca Transilvania SA to issue a card in the name of a relative, with the possibility of him accessing only the account in EURO. At the time of picking up the card, the customer and the person who had the right to operate the euro account were using a certain Internet Mobile Banking application of Banca Transilvania that allowed restricting the viewing of some accounts.

During the investigation, from the data update request (Purchase of banking products/services) for a new mobile application intended for the provision of services, it resulted that the restriction of the right to operate is still applied only to the euro account for the relative designated by the customer. In this situation, it appeared that the petitioner clearly expressed his will regarding the possibility of viewing only on the account in euros.

However, after activating the Internet Mobile Banking service to use the new application, the petitioner's relative was able to gain unauthorized access to all the holder's accounts.

As such, it was found that the operator did not prove that, at the time of using his client's data, he provided him, in a concise, transparent, intelligible and easily accessible form, information on the recipients or categories of recipients of the personal data, as provided by art. 13 para. (1) lit. e) in conjunction with art. 12 of Regulation (EU) 2016/679.

Therefore, the operator did not provide proof of informing the data subject (the client) that, within the new application, the bank data related to all his accounts were to be disclosed to the designated person (his relative).

At the same time, the following corrective measures were applied to the operator:

- to take appropriate measures to comply with the provisions of art. 5 para. (1) lit. a) and of art. 12 and 13 of Regulation (EU) 2016/679, related to the processing of personal data within the services provided to customers, including Internet/Mobile

Banking services;

-to adopt appropriate technical measures, intended to effectively implement the principles of data protection and to integrate the necessary guarantees in the processing, both at the time of establishing the means of processing, and in that of the processing itself, in order to meet the requirements Regulation (EU) 2016/679 and protect the rights of data subjects, in accordance with the provisions of art. 25 of Regulation (EU) 2016/679. In this sense, the implementation of appropriate technical and organizational measures was ordered to ensure that, in all cases, only personal data that is necessary for the specific purpose of the processing and in accordance with the manifestation of free will, specific, informed and unambiguous of the data subjects (customers).

Legal and Communication Department

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