

17.12.2020

## Penalty for GDPR violation

On 26.11.2020, the National Supervisory Authority completed an investigation at the operator Banca Transilvania SA and found a violation of the provisions of art. 32 para. (1) and (2) in conjunction with art. 5 lit. f) from the General Regulation on Data Protection.

The operator of Banca Transilvania SA was fined 487,380 lei (the equivalent of 100,000 EURO) for contravention.

The investigation was started following the receipt of notifications regarding the violation of the confidentiality and security of personal data.

It was found that there was disclosure in the public space (on-line) of the statement requested by the operator to his customer regarding how he intended to use a certain amount of money that he wanted to withdraw from his account. This statement was distributed among several employees of Banca Transilvania on their work e-mail addresses. One of the employees listed the email containing the customer statement, as well as the email containing the internal conversation between the operator's employees. Another employee took a photo of the listed entry with his mobile phone and shared it via WhatsApp.

Subsequently, the listed entry was posted and shared on the Facebook social network and on a website.

This situation led to the disclosure and unauthorized access to certain personal data (name and surname, e-mail addresses, behavioral data, personal preferences, financial transaction value, workplace address, position and place of work, telephone number of service) of 4 natural persons concerned (one client and 3 own employees), although according to art. 5 lit. f) from the General Data Protection Regulation, the operator had the obligation to respect the principle of integrity and confidentiality of personal data.

During the investigation carried out at Banca Transilvania SA, the Supervisory Authority found that the operator did not take sufficient measures to ensure that any natural person acting under the authority of the operator (employees of the operator) and who has access to personal data does not process them except at the request of the operator.

The disclosure produced in the public space also proves the inefficiency of the internal training of the operator's employees regarding compliance with the rules for the protection of personal data of the persons concerned, although the training of employees is an intrinsic part of the technical and organizational measures that the operator was obliged to adopt in order to ensure a level security corresponding to the processing risk, thus violating the provisions of art. 32 of the General Data

Protection Regulation.

In this context, it was also considered that the disclosure of personal data in the public space (on the Internet) generated a series of damages of a moral nature, as well as other significant disadvantages of an economic or social nature for the natural person affected by the occurrence of the incident of security (client of Banca Transilvania).

Legal direction and communication

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