29.08.2022

Penalty for GDPR violation

In July 2022, the National Supervisory Authority completed an investigation at the operator Alpha Bank România SA and found a violation of the provisions of art. 29 and art. 32 para. (1) lit. b), paragraph (2) and para. (4) of the General Data Protection Regulation.

As such, the operator was penalized for contravention with a fine of 4,935.10 lei (equivalent to 1000 EURO).

The investigation was started as a result of a data security breach notification that was sent by Alpha Bank Romania SA, based on the provisions of art. 33 of the General Data Protection Regulation.

Thus, according to what is mentioned in the notification form, the violation of the security of data processing occurred as a result of the fact that a document was sent to another recipient, by mistake, by using the Whatsapp application.

As part of the investigation, it turned out that this violation led to the unauthorized disclosure or unauthorized access to certain personal data, such as: name and surname, CNP, position and signature, type of credit, number and date of signing the contract, period of crediting and the date of the last due date, being affected by the incident a number of 4 natural persons concerned.

The National Supervisory Authority found that Alpha Bank Romania SA did not implement adequate technical and organizational measures in order to ensure a level of confidentiality and security corresponding to the processing risk and did not take sufficient measures to ensure that any natural person acting under the authority of the operator and who has access to personal data only processes them at his request.

At the same time, pursuant to art. 58 para. (2) lit. d) from the General Regulation on Data Protection, the following corrective measures were ordered against the operator:

- reviewing and updating 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, by implementing and transmitting to the responsible persons some instructions on the prohibition of the use of personal equipment of employees in customer relations (eg mobile phone) for communication applications/online chat services not authorized by the Bank;
- the adoption of measures regarding the training of persons acting under the operator's authority, including regarding the risks

and consequences involved in the disclosure of personal data.

Legal and Communication Department

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