16.11.2022

Sanctions for GDPR violations

In September 2022, the National Supervisory Authority completed an investigation at the operator Raiffeisen Bank SA and found multiple violations of the provisions of the General Data Protection Regulation.

The operator was penalized with two warnings and three fines totaling 138,572 lei (the equivalent of 28,000 EURO), as follows:

1. Fine in the amount of 98,980.00 RON, the equivalent of 20,000 EURO for the violation of art. 32 para. (4) in conjunction with art. 32 para. (1) and para. (2) from GDPR;

2. Warning for violating the provisions of art. 32 para. (1) and art. 32 para. (2) from GDPR;

3. Fine in the amount of 14,847.00 RON, the equivalent of 3000 EURO, for the violation of art. 32 para. (4) in conjunction with art. 32 para. (1) and para. (2) from GDPR;

4. Fine in the amount of 24,745.00 RON, the equivalent of 5000 EURO, for the violation of art. 25 para. (1) of the GDPR;

5. Warning for violation of the provisions of art. 32 para. (4) in conjunction with art. 32 para. (1) and para. (2) of the GDPR.

The investigation was started as a result of the transmission by the operator Raiffeisen Bank SA of a number of 17 notifications regarding the occurrence of personal data security violations, according to the provisions of the General Data Protection Regulation.

Thus, during the investigation, the following were mainly found:

Queries were made by Raiffeisen Bank S.A. in the records system managed by Biroul de Credit S.A., respectively in that managed by the National Agency for Fiscal Administration (ANAF), and the IT systems of the operator Raiffeisen Bank S.A. were also used. to simulate credit decisions ("prescoring") for an external credit broker.

In two situations, prescoring operations were carried out for customers or potential customers, but the query in the Credit Bureau System was carried out without the documentation related to the query being signed by the respective applicants. It was found that the incidents notified to the National Supervisory Authority concerned a number of at least 169 natural persons.

The operator of Raiffeisen Bank SA notified the Authority of an incident related to the granting of loans to some clients, natural persons, through an entity having the capacity of authorized person of the operator. The basis of the notification was information according to which customers had been approved for loans for personal needs without them having requested them and without having signed the related documents.

Therefore, it was noted that Raiffeisen Bank S.A. did not take measures to ensure that any natural person who acts under the authority of the operator and has access to personal data only processes them at the request of the operator and did not implement adequate technical and organizational measures to ensure a level of security corresponding to the risk of processing . This led to unauthorized access and/or unauthorized disclosure of personal data transmitted, stored or processed through the IT applications used by Raiffeisen Bank S.A. in lending activity.

The operator notified an incident regarding the violation of data security, which consisted in the fact that, during the process of updating the data of a client, a wrong e-mail address was entered into the system and a document with multiple data was sent to another natural person personal data belonging to the bank's client.

Another incident consisted in the fact that the Raiffeisen Bank SA operator sent confidential data via e-mail to a person other than the person concerned.

Another notification of an incident produced at the level of the operator concerned the fact that a document entitled "Form for defining personal data" was sent to an erroneous e-mail address of another natural person and which contained numerous personal data of a customer of the bank.

A similar incident occurred as a result of the fact that two clients of the operator submitted similar complaints, and when preparing the response e-mail to the first client's complaint, the operator attached documents with personal data belonging to the other client to the e-mail sent to him. The cause of the wrong transmission of the documents was represented by the similarity between the typology of notifications and the successive time of sending the response.

Another incident regarding data security violations, notified by the operator, looked at a situation involving suspicions of internal credit fraud and consisted of:

a) carrying out specific operations for granting a loan for a natural person client, without the presence of the applicant at the agency's headquarters.

b) applying for Credit Card credit facilities, completing and signing the documentation related to the credit card facility, requesting credit facilities for personal needs credit, completing and signing the documentation related to the personal needs credit facility, updating the data of the concerned persons in the Bank's application by changing the telephone number of the concerned persons with the telephone number of the bank employee and by entering a fictitious email address.

A similar incident, notified by the operator and investigated by the National Supervisory Authority, consisted in the processing

of data by the operator in connection with the granting of three credit facilities (Flexicredit, Flexicredit refinancing respectively Shopping Card), on behalf of a natural person, client of the bank, but without actually requesting those loans.

Another violation of the security of personal data, notified by the banking operator, consisted in the unauthorized disclosure of the personal data of some customers from their Smart Mobile account (the mobile banking service provided by Raiffeisen Bank) to other customers of the operator.

In the context of the above, during the investigation it was found that the operator Raiffeisen Bank S.A. has not taken measures to ensure that any natural person acting under its authority and having access to personal data does not process it except at the operator's request. This led to unauthorized access to the personal data of Raiffeisen Bank S.A. customers (for example, name, surname, home address, citizenship, nationality, person's image, personal numerical code, ID card number and series, email, no . telephone, data from the Credit Bureau System, data from the record system managed by ANAF, data from the Smart Mobile account) and upon the unauthorized disclosure of these data by the operator.

We emphasize that, according to art. 5 para. (1) lit. f) from GDPR, Raiffeisen Bank S.A. had the obligation to process personal data in a way that ensures their adequate security, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, by taking appropriate technical or organizational measures ("integrity and confidentiality").

Legal and Communication Department

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