

FIRST FINE IN THE APPLICATION OF THE RGPD

On 27.06.2019, the National Supervisory Authority completed an investigation at the operator UNICREDIT BANK S.A. and found that it violated the provisions of art. 25 para. (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation).

The operator was fined 613,912 lei, the equivalent in euros of 130,000 euros.

The sanction was applied UNICREDIT BANK S.A. due to the non-application of appropriate technical and organizational measures, both in the determination of the means of processing and in the processing itself, designed to effectively implement data protection principles, such as data minimization, and to integrate the necessary safeguards into the processing in order to meet the requirements of the RGPD and to protect the rights of data subjects. This led to the disclosure in the documents containing the details of the transactions and which are made available online to the customers receiving the payments, the data regarding the CNP and the payer's address (for the situations in which the payer made the transaction from one account opened to another credit institution - external transactions and cash deposits), respectively the data regarding the payer's address (for the situations in which the payer carried out the transaction from an account opened at UNICREDIT BANK SA - internal transactions), for a number of 337,042 persons concerned, during May 25, 2018 - December 10, 2018.

The sanction was applied as a result of a notification from the National Supervisory Authority dated 22.11.2018 stating that the data regarding the CNP and the address of the persons making payments to UNICREDIT BANK SA, through online transactions, were disclosed to the beneficiary of the transaction, through the account statement forms / details.

According to art. 5 para. 1 lit. c) of the RGPD ("Principles related to the processing of personal data"), the controller had the obligation to process data limited to what is necessary in relation to the purposes for which the data are processed.

At the same time, recital 78 of the Regulation states: "The protection of the rights and freedoms of individuals with regard to the processing of personal data requires the adoption of appropriate technical and organizational measures to ensure compliance with the requirements of this Regulation. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures that comply in particular with the principle of data protection from the time of design and the default of data protection. Such measures could include, but are not limited to, minimizing the processing of personal data, pseudonymizing such data as soon as possible, transparency regarding the functions and

processing of personal data, empowering the data subject to monitor data processing, empowering the operator to create and improve security features. When developing, designing, selecting and using applications, services and products that rely on the processing of personal data or process personal data to fulfill their role, the manufacturers of such products and the providers of such services and applications should be Encourage them to consider the right to data protection when designing and designing such products, services and applications and, taking into account the current state of development, to ensure that operators and persons empowered by operators are able to fulfill their obligations regarding data protection. The principle of data protection from the moment of design and that of implicit data protection should also be taken into account in the context of public tenders. "

Legal and Communication Office

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