25.11.2022

Fine for GDPR violation

In November 2022, the National Supervisory Authority completed an investigation at the operator OTP LEASING ROMANIA IFN SA, during which it found a violation of the provisions of art. 25 para. (1), art. 32 para. (1) lit. b) and d) and as well as art. 32 para. (2) of the General Data Protection Regulation.

The operator was fined 14,675.7 lei (equivalent to the amount of 3,000 EURO).

The investigation was started as a result of the transmission by the operator of a notification regarding the violation of personal data security pursuant to art. 33 of the General Data Protection Regulation.

In the notification sent, the operator of OTP LEASING ROMANIA IFN SA claimed that he was informed by a natural person that he was able to access the My Leasing IT platform in an unauthorized manner, by altering the URL address and creating an administrator account. Thus, he was able to access the data of the operator's customers, legal entities, who created an account on the platform in order to track information related to leasing contracts.

During the investigation, it was found that some of the operator's clients, legal entities, had registered in the platform, as contact data, email addresses that contained the name, surname, email address and telephone number of the representatives (natural persons) of these persons legal, and that data could be the data accessed in an unauthorized way on the platform (MyLeasing).

The unauthorized access to the MyLeasing system was determined by the lack of an adequate level of security, corresponding to the processing risks, which should have been ensured by OTP LEASING. Thus, the confidentiality of personal data processed through the MyLeasing platform for the natural persons concerned, registered as contact persons for the legal persons in the platform, was violated.

The OTP LEASING operator did not inform the persons concerned about the occurrence of the personal data security incident, although the data disclosed in an unauthorized manner may lead to damages to these natural persons, representatives of legal entities.

As such, the National Supervisory Authority found a violation of the provisions of art. 25 para. (1) from GDPR, art. 32 para. (1) lit. b) and d) and art. 32 para. (2) of the GDPR by OTP LEASING ROMANIA IFN SA, because this operator did not implement adequate technical and organizational measures, both at the time of establishing the means of processing and at the time of

the processing itself.

At the same time, the operator did not carry out the periodic testing, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the security of the processing, intended to effectively implement the principles of data protection and integrate the necessary guarantees within the processing, in order to meet the requirements RGPD and protect the rights of data subjects.

It was also established that the operator did not implement adequate technical and organizational measures to ensure a level of security appropriate to the processing risk, including the ability to ensure the confidentiality, integrity, availability and continued resilience of the processing systems and services.

In this context, we specify that according to Recital 78 of the RGPD "the protection of the rights and freedoms of natural persons with regard to the processing of personal data requires the adoption of appropriate technical and organizational measures to ensure the fulfillment of the requirements of this regulation. In order to be able to demonstrate compliance with this regulation, the operator should adopt internal policies and implement measures that respect in particular the principle of data protection by design and data protection by default."

At the same time, Recital 83 of the RGPD mentions: "In order to maintain security and prevent processing that violates this regulation, the operator or the person authorized by the operator should assess the risks inherent in the processing and implement measures to mitigate these risks (...). Those measures should ensure an appropriate level of security, including confidentiality. (…)When assessing the risk for the security of personal data, attention should be paid to the risks posed by data processing (…) which may lead in particular to physical, material or moral damages."

Legal and Communication Department

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