

18.05.2023

A new penalty for non-compliance with the GDPR

The National Supervisory Authority completed, in May of this year, an investigation at the operator AUTOMOBILE BAVARIA SRL and found a violation of the provisions of art. 32 para. (1) lit. b) and d), in conjunction with art. 32 para. (2) and of art. 25 para. (1) of the General Data Protection Regulation (RGPD).

As such, the operator was penalized:

with a fine in the amount of 88,563.60 lei, the equivalent of 18,000 EURO, for the violation of art. 32 para. (1) lit. b) and d), in conjunction with art. 32 para. (2) from GDPR;

with a warning for violating art. 25 para. (1) of the GDPR.

The investigation was started as a result of the transmission by the operator of a notification of a breach of the security of personal data under the General Data Protection Regulation.

The breach of data security occurred as a result of the unauthorized disclosure of personal data (name, surname, city, email address, phone number, current car model, current car year of manufacture, buy-back option, purchase term, purchase method (cash, credit, leasing), approximate available budget, marketing consent options (telephone contact, email contact, SMS contact, newsletter registration)) for a number of 290 customers/potential customers of the operator, in the period July 2022 – 04.08.2022, these data being publicly accessible on the operator's web page.

The investigation found 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 of processing systems and services and a process for periodic testing, evaluation and assessment of the effectiveness of the measures technical and organizational to guarantee processing security.

It was also found that AUTOMOBILE BAVARIA SRL did not ensure the protection of personal data, starting from the moment of conception (privacy by design) and implicitly (privacy by default), by not complying with the provisions provided for in art. 25 para. (1) of the GDPR, in the sense that it did not implement, both at the time of establishing the means of processing and at the time of the processing itself, adequate technical and organizational measures, intended to effectively implement the principles of data protection and to integrate the necessary guarantees in the processing, to meet the requirements of the GDPR and protect the rights of the data subjects.

At the same time, pursuant to art. 58 para. (2) lit. d) from the RGPD, the corrective measure was ordered to implement a plan that includes a process of periodic testing, evaluation and assessment of all systems and their subsequent modifications carried out by the operator or service providers (authorized persons), through which processing personal data, in order to guarantee the security of the processing, starting from the moment of conception and by default (privacy by design and privacy by default).

Legal and Communication Department

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