07.11.2022

Penalty for GDPR violation

In October 2022, the National Supervisory Authority completed an investigation at Compania Nationala Po□ta Română SA and found a violation of the provisions of art. 32 para. (1) lit. b) and para. (2) of the General Data Protection Regulation.

As such, Compania Na□ională Po□ta Română SA was penalized for contravention with a fine of 9,883.80 lei (equivalent to 200 EURO).

The investigation was started as a result of the fact that a data operator notified the National Supervisory Authority of the violation of data security by Compania Na□ională Po□ta Română SA, as an authorized person.

As part of the investigation, it turned out that the authorized Compania Na□ională Po□ta Română SA lost certain postal items th contained decisions establishing pension rights, work cards and death certificates, affecting 35 natural persons (addressees).

It was also found that this company did not implement adequate technical and organizational measures to ensure a level of confidentiality and security of the personal data of the data subjects, which led to the loss, unauthorized disclosure or unauthorized access to certain personal data .

At the same time, under art. 58 para. (2) lit. d) from the General Regulation on Data Protection, it was decided against the Compania Na□ională Po□ta Română SA and the corrective measure to review and update 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 personal data, in order to ensure the protection of data processed both on workstations (PCs), and for the provision of postal services in physical format (receiving or delivering postal items), as well as ensuring physical protection of the work spaces where they are processed mailings and measures regarding the training of persons acting under the authority of the company.

In this context, we specify that, according to the provisions of art. 4 point 8 of the General Data Protection Regulation person authorized by the operator is the natural or legal person, public authority, agency or other body that processes personal data on behalf of the operator.

At the same time, we specify that, art. 32 para. (1) and (2) of the General Data Protection Regulation mention:

"(1) Taking into account the current stage of development, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk with different degrees of probability and severity for the rights and freedoms of

natural persons, the operator and the person authorized by him implement adequate technical and organizational measures to ensure a level of security corresponding to this risk, including among others, as appropriate:

a) pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and continuous resistance of processing systems and services;

c) the ability to restore the availability of personal data and access to them in a timely manner in the event of a physical or technical incident;

d) a process for periodic testing, evaluation and assessment of the effectiveness of technical and organizational measures to guarantee the security of the processing.

(2) When assessing the appropriate level of security, account is taken in particular of the risks presented by the processing, generated in particular, accidentally or illegally, by the destruction, loss, modification, unauthorized disclosure or unauthorized access to the personal data transmitted, stored or otherwise processed."

In this context, we underline the fact that the obligations to ensure the confidentiality and security measures of data processing fall on both the operator and the person authorized by him.

Legal and Communication Department

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