A new sanction for violating the RGPD

The National Supervisory Authority completed, on 13.12.2019, an investigation at the operator Entirely Shipping & Trading S.R.L., finding the following:

- violation of the provisions of art. 12 and art. 13 of the General Data Protection Regulation (RGPD);
- violation of the provisions of art. 5 para. (1) lit. c), art. 6 and art. 7 of the RGPD;
- violation of the provisions of art. 5 para. (1) lit. c), art. 9 and art. 7 of the RGPD;
- violation of the provisions of art. 5 para. (1) lit. a), b) and e) and art. 6 of the RGPD.

The operator Entirely Shipping & Trading S.R.L. was sanctioned as follows:

- warning for violation of the provisions of art. 12 and art. 13 of the RGPD, as the operator did not provide evidence that it provided clear, complete and accurate information to the data subjects;
- fine in the amount of 23,893 lei, the equivalent of 5,000 euros, for violating the provisions of art. 5 para. (1) lit. c), art. 6 and art. 7 of the RGPD, as the operator has excessively processed the personal data (image) of his employees through video cameras installed in the offices where they operate and in places where there are lockers where employees store their spare clothes (locker rooms). );
- fine in the amount of 23,893 lei, the equivalent of 5,000 euros, for violating the provisions of art. 5 para. (1) lit. c), art. 9 and art. 7 of the RGPD, as the operator has processed biometric data (fingerprints) of employees and other means can be used to achieve this goal, less intrusive to the privacy of data subjects;
- warning for violation of the provisions of art. 5 para. (1) lit. a), b) and e) and art. 6 of the RGPD, as the operator illegally processed the personal data of a former employee by using them in e-mail correspondence, in order to carry out the company's activity, after the termination of the contractual relationship with him.

The sanctions were applied as a result of a complaint alleging that Entirely Shipping & Trading S.R.L. installed audio-video surveillance cameras in employees' offices, locker rooms and in the dining room and that, in certain locations (restricted access spaces), access was based on fingerprints.

It was also alleged that the operator used the identity of a former employee to send e-mails in the interest of the service without the latter having been informed in advance.

In the investigation, the following were found:

the operator has not demonstrated a legitimate interest in the video surveillance system installed at its premises, which prevails over the interests or fundamental rights and freedoms of the data subjects, has not consulted the trade union or, as the case may be, the employees' representatives. before the introduction of monitoring systems, as well as the fact that other less intrusive forms and ways of achieving the goal pursued by the employer have not previously proved effective;

the operator has not demonstrated the existence of adequate data protection policies and the implementation of appropriate technical and organizational measures to ensure a level of security appropriate to that risk;

the processing of biometric data through the access control system was not collected for appropriate purposes, relevant and limited to what was necessary in relation to the purposes for which it was processed;

the operator has not performed a data protection impact assessment.

At the same time, the following corrective measures were applied to the operator:

the corrective measure to ensure the correct information of the persons concerned by communicating in a concise, transparent, intelligible and easily accessible form all the information provided by art. 13 of the RGPD and in the conditions of transparency mentioned in art. 12 of the RGPD, as well as to modify the documents through which the information is currently provided;

the corrective measure to ensure the conformity of the personal data processing operations in the video monitoring activity, respecting the principle of “minimizing the data”;

the corrective measure to ensure the conformity of the personal data processing operations in the access control activity, respecting the principle of “minimizing the data”;

corrective action to ensure the compliance of personal data processing operations with the provisions of the RGPD, by implementing a security policy and implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risks.

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