data protection - legislative changes published in February 2022

I. ROMANIA

1. SANCTIONS APPLIED BY THE NATIONAL SUPERVISORY AUTHORITY

1.1 GRUPEX 2000 LLC was sanctioned for violating the provisions of Article 6 and Article 9 by reference to the principles highlighted in Article 5 para. (1) point a), b), c), and f) and para. (2) of the GDPR with a fine in the amount of LEI 4,943.60 (the equivalent of EURO1,000)

Following the investigation, the Data Protection Authority found that a video containing images of individuals, institutionalized pacients, had been posted on the controller's website, leading to the unlawful processing of the pacient's medical and health data.

As a corrective measure, the controller was required to implement appropriate technical and organizational measures for the processing of sensitive data, so as to ensure compliance with the provisions of the GDPR.

1.2 SABOU, BURZ & CUC Law Firm was sanctioned for violating the provisions of Article 6 in conjunction with Article 5 para. (1) point a), b), c), f) and para. (2) of the GDPR with a fine in the amount of LEI 4,946.00 (the equivalent of EUR 1,000)

Following the investigation, the Data Protection Authority found that the controller had disclosed to a 247-Member WhatsApp group, without a legal basis, excessively and incompatible with the original purpose of the processing, in the absence of technical and organizational measures for maintaining the confidentiality, personal data, such as: the first name, surname, home address and information relating to a case file pending before a court, of one of its clients.

As corrective measures, the controller was requested to notify all members of the WhatsApp group to delete the personal data disclosed and to avoid disclosure of data, except where permitted by law, including through regular training of persons processing the data under its authority.

The investigation was initiated as a result of a complaint filed by the controller's client, who reported the unlawful disclosure of personal data, without his prior consent and information.

1.3 IAMSAT MUNTENIA SA was sanctioned for violating the provisions of Article 12 and Article 13 of the GDPR with a fine in the amount of LEI 9,892.40 (the equivalent of EUR 2,000) and for violating the provisions of Article 12 para. (3) and Article 21 of the GDPR with a fine in the amount of LEI 4,946.20 (the equivalent of EUR 1,000)

Following the investigation, the Data Protection Authority found that the controller continued to process the personal data of one of its employees even after the termination of the employment contract, despite that the employee had previously stated that he does not express his consent to the use of his email address and that he opposes the processing of his data by both the controller and any other natural and/or legal persons, after the termination of his employment.

The controller also failed to settle the request of his employee and to provide him with a reply on the measures taken in response to the exercise of his right to object, within the time limits provided by law.

It was also found that the controller failed to comply with its obligation to provide prior information to its employees, before starting processing personal data by video surveillance means installed at the workplace.

As corrective measures, the controller was requested to provide the data subject with a response on his request, containing also the measures taken following the exercise of his right to object and to ensure that the data subjects, in particular its employees, are fully informed on the use of the video surveillance system at the workplace.

2. REGULATIONS

The EDPB adopts the final version of Guidelines 04/2021 on Codes of Conduct as tools for transfers, after the public consultation.

The Guide provides practical guidelines on Codes of Conduct, as appropriate safeguards for the transfer of personal data from controllers and processors to a third country or an international organization.

In light of safeguards provided by existing transfer tools under Article 46 GDPR, to be considered as providing appropriate safeguards, the Code of Conduct intended for transfers shall generally cover the following elements: a description of transfers to be covered by the code (nature of data transferred, categories of data subjects, countries); a description of the data protection principles; rights and obligations arising under the GDPR for controllers/processors, but also the guarantees that are specific to transfers.

The data exporter is not required to adhere itself to the Code of Conduct to benefit of its effects. It is sufficient that the data importer commits itself under the Code and guarantees its binding and enforceable nature, through contractual or other legally binding instruments.

The Guidelines are available at the following link:
edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf

II. EUROPEAN UNION

1. SANCTIONS GRANTED IN THE EU

1.1 The Spanish Data Protection Authority ("AEPD") imposed to Amazon Road Transport Spain S.L. a fine of EUR 2 million for breaches of the GDPR provisions

Following the investigation, it was found that the controller was requesting, from the independent contractors who were to be hired, criminal record certificates showing the absence of criminal convictions, contrary to Article 10 of the GDPR.

The fact that they were expressly required to give their consent to the transmission of personal data to group companies and suppliers established outside the European Economic Area is not likely to lead the controller being held liable under the GDPR.

As a corrective measure, the controller was required to implement technical and organizational measures to ensure compliance with the GDPR of personal data collection and processing processes and delete all personal data obtained following receipt of criminal records certificates.

1.2 The Spanish Data Protection Authority ("AEPD") imposed to Vodafone España S.A.U a fine of EUR 3,94 million for breaches of the GDPR provisions

Following the investigation, it was found that the controller failed to implement sufficient security measures to verify the identity of the SIM card holders and thus prevent their fraudulent cloning. In particular, the fraudsters managed to obtain, through Vodafone España, a reply of the SIM cards belonging to 9 targeted persons, subscribers to the company's telecommunications services.

This operation enabled bank transfers and contracts to be concluded to the detriment of the data subjects, with the greatest damage amounting EUR 17,000. It was found that any person in possession of a data subject's basic personal data could bypass the security measures to take possession of a cloned SIM card.