



data protection - legislative changes published in August 2022

I. ROMANIA

1 SANCTIONS APPLIED BY THE NATIONAL SUPERVISORY AUTHORITY (ANSPDCP)

1.1 ENEL ENERGIE MUNTENIA S.A. was sanctioned for violating the provisions of Article 32 of the GDPR with a fine amounting to LEI 49,337.00 (the equivalent of EUR 10,000)

The investigation was initiated as a result of a complaint by the data subject stating that, following a telephone request made to the controller, he/she had received an e-mail reply addressed to another customer, along with his/her documents containing personal data.

In addition, the controller has also been given a warning for failure to comply with the obligation under Article 33 of the GDPR to notify the security incident within 72 hours from the time on which it became aware.

As corrective measures, the controller was required to implement adequate technical and organizational measures to ensure a level of confidentiality and security appropriate to the risk of processing and to contact the claimant with the request to destroy the received documents.

1.2 SEPHORA COSMETICS ROMANIA S.A was sanctioned for violating the provisions Article 21 of the GDPR with a fine amounting to LEI 9,883.60 (the equivalent of EUR 2,000)

Following the investigation, it was found that the controller continued to process the data subject's personal data for marketing purposes, although the data subject had previously exercised his right to object.

Hence, the claimant continued to receive repeated SMS commercial messages, although the controller had previously informed her that her personal data would no longer be processed for this purpose.

1.3 ALPHA BANK ROMANIA S.A was sanctioned for violating the provisions Article 29 and Article 32 para. (1) point b), para. (2) and para. (4) of the GDPR with a fine amounting to LEI 4,935.10 (the equivalent of EUR 1,000)

Following the investigation, it was found that an employee of the controller had mistakenly transmitted a document containing personal data of 4 data subjects (name and surname, personal identification number, position and signature, the type of loan, the number and date of signature of the loan agreement, the loan duration and the last due date of the loan) to another recipient via the Whatsapp application, which led to a breach of personal data security.

As corrective measures, the controller was required to update and revise its technical and organisational measures by implementing instructions employees prohibiting employees from using their personal equipment in dealing with customers for communication applications/online chat services not authorised by the Bank.



II. EUROPEAN UNION

1 SANCTIONS APPLIED IN THE EU

1.1 The French Data Protection Authority ("CNIL") imposed to Accor SA a fine of EUR 600,000 for breaches of the GDPR

Following the investigation, the CNIL found that once a reservation was made via the controller's website, data subjects automatically became subscribed to a newsletter containing commercial offers from the controller's partners, with the box referring the consent to receive marketing messages being ticked by default.

Technical difficulties which did not allow exercising the right to object on receiving marketing messages were also identified.

The investigation was initiated following multiple complaints received by National Supervisory Authorities in the EU.

1.2 The Italian Data Protection Authority ("Garante") imposed to UniCredit S.p.A a fine of EUR 70,000 for breaches of the GDPR provisions

Following the investigation, Garante found that the controller's refusal to respond to the data subject's request for access to his or her personal data collected was not justified.

Following the investigation, Garante found that the refusal of the controller to respond to the data subject's request for access to his/her personal data, due to the failure to use a standard form provided by the controller, was not justified.

Hence, preparing a standard form by the controller may be an organizational measure designed to facilitate the procedure, but making the exercise of the right of access conditional on its completion and refusing to consider requests submitted in another form, is a violation of the GDPR provisions.

1.3 The Norwegian Data Protection Authority ("Datatilsynet") imposed to Recover AS a fine of EUR 20,000 for breaches of the GDPR

Following the investigation, Datatilsynet found that the controller processed personal data in the absence of any contractual relation with the data subject.

The data subject complained that he had received, in the absence of a prior request and without any type of relation with the controller, a credit score, the granting of which involved the analysis of various documents containing personal information on the person's financial situation such as payment notices, loan instalments, debts and so on.