data protection - legal changes published in May 2021

I. Romania – sanctions

1. ANSPDCP. World Class Romania S.A. was sanctioned for violating the provisions of General Data Protection Regulation with a fine in the amount of RON 9,851 (the equivalent of the amount of EUR 2,000)

During the investigation started following the receipt of a complaint, the National Supervisory Authority found that the controller ***World Class Romania S.A. posted on the WhatsApp group of its employees a resignation request of one of its employees***, thus allowing unauthorized access of all members of that WhatsApp group to certain personal data (name, surname, address, serial number and identity card, code personal information, information related to the request for termination of employment).

Also, ***a corrective measure*** was also applied to the controller World Class Romania S.A. Thus, within 30 days from the date of communication of the minutes, the controller was ordered to ensure compliance with the General Data Protection Regulation, personal data processing operations, by implementing appropriate technical and organizational measures in case of remote transmission of personal data, including in terms of regular employee training.

2. ANSPDCP. Telekom Romania Communications S.A. was sanctioned with a warning and a fine in the amount of RON 9,851.40 (equivalent to the amount of EUR 2,000)

The sanctions were applied following a complaint alleging that ***the petitioner had been contacted on his telephone number for marketing purposes by a Telekom representative, although he had withdrawn his consent*** to the use of his personal data upon termination of the relationship. contractual with the operator.

Subsequently, the petitioner ***exercised his right to object*** to the processing of his personal data for marketing and advertising purposes by requesting to the controller to delete his telephone number and e-mail address from Telekom's database.

However, ***the petitioner was contacted again by a Telekom representative for marketing purposes***. Thus, the petitioner sent the controller a new request not to be contacted and to have his telephone number and e-mail address deleted from the database.

Following this request, the controller informed the applicant that his e-mail address and telephone number had been deleted from the customer management system, confirming, at the same time, that he had been called by a Telekom representative, who, due to a human error, he did not realize that he did not have the petitioner's permission to call him.

3. ANSPDCP. A natural person, as a controller, was sanctioned with a fine in the total amount of RON 974.89 (equivalent to the amount of EUR 200)

The investigation was started as a result of receiving several notifications complaining that through the *website https://declaratieppr.ro, by filling in a form that generates a statement on their own responsibility necessary to leave the home during the state of emergency*, they processed certain personal data, namely name, surname, parents' first name, domicile, personal numerical code, series and number of the identity document, the address of the house in fact, the place of travel, the purpose of the trip and the signature.

During the investigation, the National Supervisory Authority found that the ***controller did not present evidence to show that he had legally processed personal data***, collected and stored on the website https://declaratieppr.ro.

At the same time, it was found that ***the controller did not present evidence showing that he provided information to the data subjects*** about the processing of their personal data, collected on the same site.

Also, the controller (natural person) ***did not take adequate security measures*** to ensure that the file containing the personal data of the data subjects is not subject to processing risks, generated in particular, accidentally or illegally, by destruction, loss or loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.

4. ANSPDCP. Banca Comercială Română S.A. was sanctioned with a fine of a total amount of RON 9,855.8 (equivalent to EUR 2,000)

The investigation was initiated following the receipt of a complaint alleging that Banca Comercială Română S.A. ***used, without consent, the personal data of a natural person, in enforcement proceedings for debts resulting from a credit agreement of which he was unaware***.

The petitioner therefore complained about the unauthorized use of his personal data for purposes other than those authorized by him, as well as the use of an address that was no longer relevant and for which the petitioner considered that the bank had illegally accessed a database. He also complained about the lack of information regarding the source of collecting this information according to art. 14 of the GDPR, as well as the failure to receive a response regarding several requests addressed by it to BCR S.A.

During the ANSPDCP investigation, it was found that ***Banca Comercială Română S.A. processed the personal data of the petitioner without legal grounds, by erroneously assigning the status of guarantor in 2019, extracting outdated data, using and disclosing his personal data, in notification procedures carried out through a bailiff, regarding arrears to a credit agreement accumulated by a company, client of the bank, with which the petitioner had no relationship, in violation of art. 5 para. (1) lit. a) and d) and art. 5 para. (2), as well as of art. 6 of the GDPR***.

The National Supervisory Authority applied to the controller Banca Comercială Română S.A. and the ***corrective measure*** to ensure compliance with the GDPR of the operations of collection and further processing of personal data, by implementing effective methods of respecting the exact and current nature of the data, from the moment of data collection and their entry in the controller's database throughout the processing period.

5. ANSPDCP. Vodafone Romania S.A. was sanctioned with a fine of RON 5,000

The investigation was initiated as a result of a ***notification of personal data breach*** that was transmitted by the controller, based on the provisions of art. 33 of the General Data Protection Regulation.

It was found that ***the related invoices of some Vodafone customers were erroneously sent to the e-mail addresses of third parties.*** This led to the processing and unauthorized access to certain personal data of Vodafone customers, such as name, surname, telephone number, customer code, address.

Therefore, the National Supervisory Authority found that the controller did not take adequate technical and organizational measures to ensure the security of the processing of personal data, ensuring that personal data can be accessed only by persons authorized for the purposes authorized by law and protect personal data stored or transmitted against unlawful processing, access or disclosure.

6. ANSPDCP. An Owners Association from Iași was sanctioned with a fine of a total amount of RON 2,463.3 (equivalent to EUR 500)

The investigation was carried out as a result of a complaint alleging that ***the controller displayed the payment lists detailing the name and surname of each member of the Owners Association***. The petitioner also complained about the ***posting of a defamatory document in which his personal data*** (name and surname) were mentioned.

As the controller did not respond to the Authority's requests, although he confirmed their receipt, he was fined.

7. Summary of ANSPDCP activity - the first four months of 2021

In the first four months of 2021, the National Supervisory Authority received ***1733 complaints, notifications and notifications regarding security incidents***, based on which ***288 investigations*** were opened.

As a result of the investigations, ***15 fines were applied in the total amount of RON 110,545.7.***

Also, ***37 warnings*** were applied and ***30 corrective measures*** were ordered.

In the first four months of 2021, regarding the activity of solving complaints, the Supervisory Authority received ***1600 complaints***, on the basis of which ***155 investigations*** were initiated.

Regarding ***the security incidents***, during the period considered the data operators transmitted, both under the GDPR and Law no. 506/2004, ***84 notifications, and the notifications regarding possible non-compliances with the provisions of the GDPR amounted to 49***.

As a result of the notifications received and the security breaches notified by the controllers, during the first four months of 2021, ***133 investigations were initiated ex officio*** at the level of the Supervisory Authority.

At the same time, ***352 requests were submitted to our institution for various points of view*** regarding the interpretation and application of Regulation (EU) 679/2016 and other incidental regulations, by controllers and their processors, in the field of public and private, by other entities as well as by individuals.

We also mention that ***15 requests*** were received under Law no. 544/2001, mainly ***from the media***.

Regarding the activity of representation in court, in the first four months of 2021, the National Supervisory Authority managed a total of ***98 cases pending before the courts*** at various stages of proceedings. During the same period, ***5 new requests*** for summons were received, which had as object the contestation of the minutes of contestation / sanctioning of the contraventions concluded by the National Supervisory Authority.

II. European Union – regulations

1. Forty-ninth Plenary Session of the European Data Protection Board

At the Plenary Session of the European Data Protection Board, held online on 19 May 2021, the following were mainly adopted:

- Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority on the "*EU Code of Conduct on Data Protection for Cloud Service Providers*", presented by Scope Europe;
- Opinion 17/2021 on the draft decision of the French Supervisory Authority on the European Code of Conduct presented by cloud infrastructure service providers (CISPE);
- Declaration on the Law on data governance in the light of legislative developments;
- Recommendations on the legal basis for storing credit card data for the sole purpose of facilitating additional online transactions;
- Opinion 18/2021 on the draft standard contractual clauses (Article 28 (8) GDPR).

More information is available at: https://edpb.europa.eu/news/news_en

III. European Union – sanctions

1. The Norwegian Data Protection Authority has notified Disqus Inc. (Disqus) that intends to impose a fine of NOK 25,000,000 for non-compliance with the GDPR rules on accountability, legality and transparency

Disqus is an American company owned by Zeta Global. The company offers a public online comment sharing platform, which was previously used by a number of Norwegian online newspapers and also provides scheduled advertising services.

The Norwegian Data Protection Authority was informed about this issue through the news articles of the Norwegian National Broadcaster (NRK). According to NRK, Disqus illegally tracked visitors to Norwegian sites using the Disqus plugin. Their data was then disclosed to third-party advertising partners. NRK also wrote that this happened because Disqus did not know that GDPR applied in Norway, which was confirmed by Disqus' parent company, Zeta Global, in an interview.

Disqus argued that their practices could be based on the test of the legitimate balance of interests as a legal basis, despite the fact that the company does not know that GDPR applied to the data subjects in Norway.

2. The Icelandic Data Protection Authority fined InfoMentor for violating the provisions of the GDPR with a fine of EUR 23,100

The Icelandic authority fined InfoMentor for failing to ensure the correct security of personal data within the Mentor system, an information system for schools and other entities working with children.

Due to a vulnerability that led to the visibility of each user's six-digit number in the URL of a specific page in the Mentor system, unauthorized persons gained access to the national identification numbers and avatars of over 400 children. The incident was reported as a data breach in February 2019.

InfoMentor acknowledged that the company was aware of the vulnerability and that a solution had already been created. Due to a human error, the solution was not fully implemented in the system until the data breach occurred. InfoMentor also incorrectly sent national identification numbers of students affected by data breaches to the wrong schools and the data protection officer.

3. The Finnish Data Protection Authority has fined ParkkiPate with a fine of EUR 75,000 for breach of the provisions on the processing of personal data

The Authority received several complaints regarding the activities of the controller. Those who complained to the Authority requested information from the controller, inter alia, the source of their personal data and the basis for their processing. In addition, the applicants had requested access to or deletion of their data.

The controller refused to deliver the data until it verified the identity of the applicant. For this verification, the controller asked those requesting to disclose information such as their personal identity codes and addresses. The operator considered that it could not sufficiently identify the parking tickets in question only by the names of the persons concerned and the case numbers assigned to the parking ticket. However, the data originally held by the controller did not include personal identity codes, so it could not have compared a personal identity code provided by a data subject with the data already in its possession.

4. The Dutch Data Protection Authority fined Locatefamily.com a fine of EUR 525,000

The site publishes people's addresses and phone numbers, often without their knowledge. Anyone who wanted to remove the details from the site could not do so easily, because Locatefamily.com does not have a representative in the EU. The lack of a representative in the EU is a breach of the General Data Protection Regulation (GDPR) and is the reason why the fine was imposed.

5. The Norwegian authorities fined the electricity company Dragefossen a fine of EUR 15,000

The electricity company had a panoramic webcam mounted above its office building in the center of Rognan, with a panoramic facility. The images were streamed live on YouTube and on the company's own website. Until the Authority contacted the company, it was possible to run live stream recordings for up to 12 hours.

The area captured by the webcam included public roads, car parks and entrances to two supermarkets, a pharmacy, the local bank, the town hall and a number of other buildings.

6. The Norwegian authorities have fined the Municipality of Asker with a fine of EUR 100,000

The municipality has been fined for publishing confidential personal data and national identity numbers (NID) on its website.

On 19 May 2020, the Council was notified by a citizen that the titles of the documents relating to a total of 170 entries in the Council's correspondence diary contained 127 names and NIDs. Visible data included the title of the document, in addition to names and NIDs. The data were visible on the municipality's website for a year.

7. The Norwegian authorities sanctioned a company with a fine of EUR 25,000 for illegally forwarding an employee's emails

The name of the company was not publicly disclosed to protect the identity of its employees.

The investigation came as a result of a complaint from someone who found that his employer had started sending emails automatically.

The employer has asked the employee to set up automatic forwarding from the email account to a third-party email account for operational reasons.

8. The Norwegian authorities sanctioned the municipality of Ålesund for using the Strava application

At two schools in Ålesund, teachers asked students to download the Strava fitness app to use during their physical education lessons. Students were then given assignments, while teachers used the application tracking feature to check that all students had completed the assigned tasks.

The download of the application was mandatory and was downloaded on students' private mobile phones. The use of the tracking function must be considered as the processing of personal data.

9. The Norwegian authorities fined Basaren Drift AS with a fine of EUR 20,000 for illegal CCTV monitoring

After investigating a complaint concerning CCTV surveillance of a restaurant, the Norwegian Data Protection Authority concluded that Basaren had no legal basis for its surveillance.

The illegal CCTV surveillance targeted the employees, the rooms covering the relaxation areas of the guests in the restaurant. Restaurant guests have a legitimate expectation not to be filmed while dining there. In places used for relaxation, recreation and social gatherings, the privacy of guests must therefore be given considerable weight.

10. The Spanish authority sanctioned EPD Comercializadora, S.A.U. with a fine in the amount of EUR 1,500,000 Euros

The Authority considers that EDP COMERCIALIZADORA, S.A.U has not adopted technical and organizational measures to verify whether a person who contracts his services on behalf of another natural person is authorized to perform the contracting. Nor has it adopted technical and organizational measures to verify whether the person acting on behalf of another natural person is authorized by that person to consent to

other processing of personal data on their behalf. These consents were requested during the recruitment procedure, for two purposes: to send their own commercial and third-party communications and to profile information from third-party databases for automatic decision-making, to send personalized commercial proposals and to allow certain services to be contracted.