data protection - legal changes published in June 2021

I. Romania - sanctions

1. ANSPDCP. La Santrade S.R.L. was sanctioned for violating the General Regulation on Data Protection by a fine of RON 9,839.4 lei (equivalent to EUR 2,000)

In the investigation initiated following a complaint, La Santrade S.R.L. failed to comply with the request for information from the Authority.

The Authority also found that the controller did not take measures to ensure the effective exercise of the rights of data subjects, which led to the data subject's request for deletion of his personal data not being resolved.

Two corrective measures were also applied:

a) informing the data subject about the measures adopted regarding the deletion of the data collected without his / her express consent;

b) facilitating the exercise of the rights of data subjects, by providing valid contact data, including a functional e-mail address, which will be made public the operator's weight in the sections on personal data processing, privacy policy, contact data.

2. ANSPDCP. Dreamtime Call S.R.L was sanctioned by a fine in the amount of RON 9,852.2 (equivalent to EUR 2,000)

The investigation was initiated following a complaint alleging that SC Dreamtime Call S.R.L. illegally processed the personal data of a natural person (telephone number), by repeatedly contacting him by telephone, without prior consent.

As the controller failed to respond to the Authority's requests, although it confirmed their receipt, it was fined.

The controller was also required to provide the Authority with all requested information within 5 working days of the communication of the minutes.

II. EUROPEAN UNION - regulations

1. Plenary of the European Data Protection Board

The following documents were, *inter alia*, adopted at the Plenary of the European Data Protection Committee, held online on June 18, 2021:

- **Joint opinion with EDPS on the draft Regulation of the European Commission on the establishment of harmonized regulations on artificial intelligence**;
- **Recommendations no. 1/2020 on additional transfer measures** (final version).

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

2. Transfer of personal data from the EU to the United Kingdom

On Monday, June 28, 2021, the European Commission adopted ***two adequacy decisions for the United Kingdom***: under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive, according to a statement.

Personal data may be transferred freely from the European Union to the United Kingdom when it enjoys a level of protection essentially equivalent to that guaranteed by Union law.

Adequacy decisions also facilitate the proper implementation of the EU-UK Trade and Cooperation Agreement, which provides for the exchange of personal information.

Transfers for immigration control purposes in the United Kingdom are excluded from the scope of the GDPR's adequacy decision to reflect the recent ruling of the Court of Appeal in England and Wales on the validity and interpretation of certain restrictions on the protection of human rights data in this area. The Commission will reassess the need for this exclusion once the situation has been remedied under UK law.

III. EUROPEAN UNION - sanctions

1. France. IKEA France was fined 1 million Euros for spying on employees

On Tuesday, June 15, 2021, a court in France fined the furniture company IKEA by 1 million Euros, after proving that the ***retailer was spying on its employees and incorrectly storing their personal data***.

The French subsidiary of the Swedish company has been accused of spying on its employees for several years and violating their privacy by examining bank account records and sometimes by using fake employees to write reports about staff.

At the same time, Jean-Louis Baillot, former executive director, was sentenced to two years in prison with suspension and was fined EUR 50,000 for storing personal data of employees.

IKEA Retail France strongly condemned these practices, apologized and implemented a major action plan to prevent their recurrence.

2. USA. Volkswagen security breach

Volkswagen's U.S. division has announced that the personal data of more than 3.3 million customers and potential buyers of Audi in North America has been compromised following a security breach.

Volkswagen Group of America said that an unauthorized third party obtained some information about customers and potential buyers from a dealer for its Audi and Volkswagen brands and some dealers in the US and Canada.

3. The Icelandic data protection authority sanctioned an ice cream company for video monitoring of employees with a fine of EUR 34,000

One of the company's employees filed a complaint with the Icelandic Authority regarding an area used by employees to change their work uniform, which is under constant video surveillance. The employee also complained that he did not receive any notifications or information regarding the supervision and lack of labelling and signalling.

For security reasons, five surveillance cameras recording employees and customers were installed in the company's ice cream zone. The Icelandic authority confirmed after an inspection that the employees did not have access to an acceptable area for changing clothes, an area that is not supervised.

4. The Norwegian Data Protection Authority fined BRAbank EUR 40,000

This case concerns the insufficient assessment and testing of risks in connection with the launch of a client portal for banking services. Some clients were able to see loan information about other clients when they launched "My Page". "My Page" is a solution where clients can view information about their loan agreements.

Some clients also gained access to another client's address information, and some gained access to the wrong loan information. The incident took place at a time when "My Page" was launched to a selection of 500 bank customers.

5. The Italian authority requested the holder of the 'IO' application (PagoPA) to implement additional protection measures

Following the intervention of the Italian Authority, the controller PagoPA developed several technical measures to protect the confidentiality of the users of the "IO" application. These measures will be implemented in the new version of the application, which will be launched soon.

In view of the new measures to be taken by the company, the Italian Authority decided that the order restricting the processing issued by it could be lifted. The processing involved interactions with Google and Mixpanel. The decision was made following the exchanges with PagoPA and the efforts made by the company to remedy in a timely manner the deficiencies that the Authority has recently highlighted, so as to comply with the imposed measures.

However, processing will continue to be limited to the data collected and stored by Mixpanel. This data can no longer be used and will be stored by the company only until the Authority completes its investigations.

6. The Norwegian authorities have fined the Norwegian Sports Confederation with a fine of EUR 125,000

The sanction was imposed because personal data about 3.2 million Norwegians were available online for 87 days, due to an error in testing a cloud computing solution. Types of personal data made public included name, gender, date of birth, address, telephone number, e-mail address and affiliation with the association. Of the 3.2 million people affected by this discrepancy, 486,447 were children between the ages of 3 and 17.

7. The Swedish authorities fined the Stockholm Region with a fine of EUR 49,740 and of the 2 regions with a fine of EUR 24,871 each

The sanctions were applied as a result of an incident in which telephone calls recorded to the medical consultation service, 1177, were available unprotected on the internet.

The cause of the incident was a storage unit attached to the network that was configured incorrectly and was thus accessible on the Internet. In addition, the unit did not use encrypted communications.

8. The Dutch authority fined an orthodontic clinic with a fine of EUR 12,000

The sanction was applied because the clinic allowed new patients to register on an unsecured website. As a result, patients' sensitive personal data, such as their number of citizen services, could have fallen into the wrong hands.

The web form that the new patients registered contained mandatory fields that required all kinds of personal data, as well as data on the patient's parents, the general practitioner, the dentist and the insurance company. Most orthodontic patients were children, and this case concerned the personal data of children who need additional protection.

9. The Austrian authority sanctioned a controller for refusing to provide information

The alleged controller was requested to provide information regarding an alleged breach of the GDPR. Despite being asked several times, the alleged controller ignored all the requests made by the Authority and even refused to appear before it when he was sent to trial for an oral examination and when he was threatened with a hearing. a fine of EUR 500 if it does not appear. Consequently, the Authority requested the local authority to collect the fine. When faced with this fine, the alleged controller finally provided the requested information.

10. The Netherlands authority sanctioned CP&A with a fine of EUR 15,000

The CP&A maintenance company was sanctioned for violations regarding the processing of health data of sick employees. CP&A kept a register of the causes of sick leave. In doing so, the company processed more health data than allowed by law. In addition, the registration of sick leave was not adequately ensured. CP&A has stopped this practice.

11. The Italian authority imposed a temporary restriction on the "Mitiga Italia" application

The application was first used on May 19, 2021 to allow certified spectators who were vaccinated, recovered or with negative results for COVID-19 to enter the stadium where the final Coppa Italia football match was to take place.

The restraining order proved necessary, as the application will likely be used in the coming days to regulate access to other events, shows or sporting activities.

The Order of the Italian Authority recalls that there is currently no valid legal basis for the processing of data carried out through the application to determine the refusal of access to persons participating in sports or any other public events or accessing open rooms - partly considering that information is involved. sensitive, such as health data.