data protection - legal changes published in November 2020

I. ROMANIA - regulations

1. Processing of personal data by owners' associations

Following the views requested of the Supervisory Authority by the owners' associations regarding the data processing they carry out or intend to carry out, the Authority has issued a statement on the **purposes for which these entities collect and process personal data**, respectively:

1) Regarding the ***installation of a video surveillance system by the owners' association***, it is done based on the ***legitimate interest*** of the association, e.g. to ensure the security and protection of persons, goods and values, of buildings and public utility installations, as well as of the enclosures affected by them. Arguments regarding the justification of the legitimate interest must be found in documentation at the level of the owners 'association and, subsequently, the decision to install such a system must be adopted at the general meeting of the owners' association, according to the law.

   Regarding the installation of video cameras on each level of the building, the Authority appreciates that for the processing of the respective images it is necessary to obtain the consent of each tenant on the respective level / level.

2) Regarding the ***disclosure of data such as the name and surname of the owners / tenants on the notice board of the block staircase***, we specify that in the absence of an express legal provision the data may be disclosed only on the basis of the ***consent*** of the data subject.

3) With regard to the ***registration of personal data in the real estate book***, insofar as there is a ***legal obligation*** in this respect, the data may be processed without the consent of the data subject.

Regarding the **security measures** that the owners' association is obliged to adopt, the Authority also recommends the **pseudonymization and encryption** of personal data.

With regard to the **transparency of the processing**, in terms of **informing** the data subjects, the owners' association must carry out the information regardless of the basis of the processing. For information, one can use a ***generic information method***, by ***displaying the information note on the block staircase notice board*** or ***appropriate icons, such as in the case of video surveillance***, the information notes of the person concerned (displayed), and to other modalities (by email) that are established by the association depending on the concrete situation of data processing.

Regarding the **appointment of a data protection officer, they are not obliged to appoint a data protection officer**.

2. ANSPDCP - The Court of Justice of the European Union has confirmed the position of ANSPDCP towards Orange Romania regarding the storage of identity cards

In the dispute pending before the Romanian courts, having as parties Orange Romania SA and the National Authority for Supervision of Personal Data Processing (ANSPDCP), the Court of Justice of the European Union confirmed the position of ANSPDCP regarding the illegality of Orange Romania SA's storage of children identity documents of its

customers, without their express consent, on the occasion of concluding contracts for the provision of telecommunications services.

Orange Romania SA, by ***collecting and storing copies of identity documents***, requested by electronic communications service contracts, has excessively processed personal data falling under art. 8 of Law no. 677/2001, without the express consent of the persons concerned, express legal provisions or the approval of ANSPDCP.

In view of the above, the CJEU issued a press release which can be accessed at the following link: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-11/cp200137ro.pdf.

II. Romania - sanctions

1. ANSPDCP. DADA CREATION was fined EURO 5,000 for disclosing and unauthorized access to personal data

On November 24. 2020, the Authority issued a statement on the completion of an investigation at the operator DADA CREATION S.R.L. which was sanctioned with a ***fine in the amount of RON 24,272.50***, the equivalent of EURO 5,000 and ***warning***.

The investigation was initiated following a complaint alleging that ***a document on the detailed records of transactions received by this site from its customers (individuals) was available through the operator's website,*** document containing e-mail addresses, numbers telephone number, name and surname of customers (adults and minors), age of minors, delivery addresses, order number, total order amount, products ordered and date of order.

The operator was sanctioned with a ***warning*** because ***it did not notify the Supervisory Authority of the security incident*** (which was brought to its attention by the Authority).

2. ANSPDCP. Vodafone Romania was fined EURO 4,000 for failing to resolve the request of a data subject

On November 23, 2020, the Authority announced that it sanctioned the operator ***Vodafone Romania SA*** with a ***fine in the amount of RON 19468.8, the equivalent of the amount of EURO 4,000.***

The sanction was applied as a result of complaints claiming that the operator did not respond to requests to exercise the rights of access and deletion provided by art. 15 and art. 17 of the General Data Protection Regulation.

III. EUROPEAN UNION – regulations

1. The fortieth Plenary Session of the European Data Protection Board

On Tuesday, October 20, 2020, the 40th Plenary Session of the European Committee for Data Protection took place online, a body with legal personality of the European Union, established pursuant to art. 68 of the General Regulation on Data Protection, according to a statement.

Within this, it was adopted **Guide no. 4/2019 on Art. 25 of the General Regulation on Data Protection - ensuring data protection from the moment of conception and implicitly (privacy by design and by default).**

The adopted guide is intended to support operators and processors, in order to ensure a uniform and effective application of the requirements of this principle, taking into account the purpose, nature, context and risks of processing, in relation to the need for effective and other compliance, principles of personal data processing.

This tool contains numerous practical examples and a section of recommendations, including on the role of the data protection officer in the operators / processors.

2. The forty-first Plenary of the European Data Protection Board

The following documents were adopted at the Plenary Session of the European Data Protection Board, held online on 9 and 10 November 2020:

- Recommendations no. 1/2020 on measures supplementing transfer instruments to ensure compliance with the level of EU protection, following the Decision of the Court of Justice of the European Union in the Schrems;
- Recommendations no. 2/2020 on European Essential Guarantees regarding surveillance measures, related to the transfer activity, document with complementary role;
- The first decision pursuant to art. 65 of the GDPR, regarding the draft decision of the DPA Ireland on International Twitter.

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

3. The forty-second Plenary of the European Data Protection Board

At the Plenary Session of the European Data Protection Board on 19 November 2020, ***two new sets of draft standard contractual clauses (SCC)*** were presented, and the EDPB adopted a ***statement on the future ePriavacy Regulation.***

The European Commission has presented two SCC projects: one set of ***SCC for contracts between operators and processors and another for data transfers outside the EU***. In addition, the Commission presented another set of SCCs for the transfer of personal data to third countries in accordance with art. 46 (2) (c) GDPR. These SCCs will replace the existing SCCs for international transfers that were adopted on the basis of Directive 95/46 and needed to be updated to align them with the requirements of the GDPR as well as the CJEU's Schrems II judgment and to better reflect the use of large-scale new and more complex processing operations often involving multiple data importers and exporters. The Commission requested a joint opinion from the EDPB and the AEPD on the implementing acts for both sets of SCC.

The EDPB has adopted ***a statement on the future ePrivacy Regulation*** and the future role of supervisors and the EDPB in this context. The EDPB expressed concern about some new directions in the Council's discussions on the application of the future ePrivacy Regulation, which could lead to fragmented supervision, the complexity of procedures and a lack of coherence and legal certainty for individuals and companies.

IV. EUROPEAN UNION - sanctions

1. The Norwegian authorities have fined Østfold HF Hospital with a fine of EUR 70,000

The sanction was applied because in the period 2013-2019, the hospital stored extracts from patients' reports outside the safety zone. The case began with a notification of personal data breach from the hospital.

The Norwegian Data Protection Authority considers that Østfold HF Hospital has not established an access control system that is sufficient to prevent data breaches and that special reference is made to routines for access control and personal data storage.

2. The Spanish authority fined Telefónica Móviles España with a fine of EUR 75,000

The Spanish data protection Authority fined Telefónica Móviles España, S.A.U. with a fine of EUR 75,000 for the illegal processing of the applicant's personal data by issuing several invoices to him for services provided to a third party.

The Authority considered that the processing of the petitioner's personal data had been carried out without any legal basis and consequently fined the controller.

3. The Belgian authority fined a natural person Euro 1,500 for video surveillance

Two plaintiffs have filed a complaint with the Belgian on the video surveillance system of the two neighbors and the continued use of images made by the system. The two defendants had installed a video surveillance system with five surveillance cameras (24/7 filming) on their private property. Two cameras mentioned in the complaint were positioned in such a way that those cameras filmed the applicants' public road or private property and filmed at least one of the applicants as they drove on the public road or entered their private property.

The images were used by the defendants in a dispute procedure between the defendants and the applicants regarding environmental planning.

The Belgian authorities considered that there were legitimate interests for the defendants to protect their own private property, but the filming of large parts of the public road, as well as the filming of the applicants' private property, were not necessary to protect those legitimate interests.

4. Italian authority fined Vodafone € 12 million for aggressive telemarketing practices

The Italian authority ***fined Vodafone more than 12,250,000 euros*** for illegally processing the personal data of millions of users for telemarketing purposes. In addition to having to pay the fine, the company must implement several measures established by the Authority to comply with national and EU data protection legislation.

The Authority established that false telephone numbers or numbers not registered with the ROC (ie the Consolidated National Register of Communications Operators) were used to make the marketing calls. This practice is at the center of Vodafone's attention and is apparently linked to a shady set of unauthorized call centers that conduct telemarketing activities, regardless of personal data protection legislation.

Vodafone uses contact lists purchased from external suppliers. These lists were obtained by Vodafone business partners from other companies and were transferred to Vodafone without user consent.

Security measures for managing customer resources have also proved inadequate. In this regard, several complaints and alerts were sent to the Authority by customers who had been contacted by operators claiming to act on behalf of Vodafone and requested that they be sent IDs via WhatsApp - quite likely for spam, phishing purposes or other fraudulent activities.

In the light of the infringements found during the procedure, the Italian Authority imposed a fine of EUR 12,251,601.00.

5. The Swedish authority has sanctioned the Stockholm Education Council

The Swedish data protection authority has investigated the so-called school platform, the IT system used for the administration of students in schools in Stockholm. The analysis shows an insufficient level of security of such a serious nature that the Authority issues an ***administrative fine of SEK four million*** against the Stockholm City Council of Education.

The Swedish Data Protection Authority has received a number of notifications of personal data breaches. All incidents relate to the school platform, which is the IT system used, among other things, for the administration of students in Stockholm. The school platform contains information for up to ***500,000 students, tutors and teachers***.

Following the investigation, it was found that a large number of staff were able to access information about students with protected identities. In another situation, tutors were able to access information about other children related to, for example, grades and assessment. Through the Google search engine, it was possible to find links to connect to an administration interface where information about teachers with protected identities was accessible.

Swedish data protection authority imposed an administrative fine of SEK four million for the infringements found.

6. The Swedish authorities fined the town of Gnosjö for illegal video surveillance in a house

The Swedish Data Protection Authority imposed an administrative fine of SEK 200,000 on the municipality of Gnosjö for illegal video surveillance in an LSS home. The Swedish Data Protection Authority has received a complaint from a relative of a resident of a residential care home for people with certain functional disabilities (so-called LSS housing) in the municipality of Gnosjö, claiming that the resident is being monitored illegally.

The Gnosjö Social Assistance Committee, which is responsible for the LSS housing, said that the resident's disease profile created major difficulties for both the resident and the staff, and that there were situations where there was a risk to the resident's life and health. There were also situations in which the staff suffered injuries.

The Swedish Data Protection Authority concludes in its decision that there is no legal basis for video surveillance, that an impact assessment has not been carried out before the initiation of video surveillance and that the operator has not clearly informed about video surveillance. For these reasons, the Swedish Data Protection Authority issues an administrative fine of SEK 200,000 against the Social Assistance Committee.