data protection - legislative changes published in November 2021

I. ROMANIA

1. SANCTIONS APPLIED BY THE NATIONAL SUPERVISORY AUTHORITY

1.1 ANSPDCP. S.P.E.E.H. Hidroelectrica S.A. was sanctioned for violating the provisions of Article 32 para. (1) lit. b) and para. (2) of the GDPR with a fine in the amount of LEI 24,739.50 (the equivalent of EUR 5,000)

Following the investigation, the Data Protection Authority found that the controller did not implement appropriate technical and organizational measures to ensure a security level corresponding to the risk envisaged by the processing, which resulted in the unlawful accessing or disclosure to wrong recipients of the personal data of 325 targeted persons.

At the same time, it was found that the processing of personal data of three of the company's clients was performed after they had exercised the right to erasure their data and withdrawal their consent for the processing. For the violation of the provisions of Article 5 para. (1) lit. a) and Article 6 para. (1) of the GDPR, the controller was sanctioned with a reprimand.

The following corrective measures were applied to the controller:

- the review and update of the security and organizational measures implemented as well as the implementation of some measures regarding the periodic training of the persons acting under its authority, regarding the obligations incumbent on them according to the GDPR;
- the identification and implementation of some measure to ensure that the personal data processed are accurate and updated, considering the purposes for which they are processed.

The investigation was initiated as a result of several notifications of personal data breaches that were transmitted by the controller, based on the GDPR.

1.2 ANSPDCP. IKEA ROMÂNIA S.A. was sanctioned for violating the provisions of Article 32 para. (1) lit. b) and para. (2) of the GDPR with a fine in the amount of LEI 4,948.80 (the equivalent of EUR 1,000)

In the investigation, the Data Protection Authority found that the controller has organized a drawings contest at which the children of the Ikea Family members participated. The participants have uploaded on the online platform dedicated to the members their own drawings, together with the participation forms that contained their personal data, the data of the parents/legal guardians, inclusive their consent.

Following the investigation, it was found that the data breach incurred resulted in the unauthorized disclosure of the personal data of the Ikea Family members (first name, last name and age of the children, first name, last name, city, country, e-mail address, Ikea Family member number and holographic signature of the parent/legal guardian) on the online platform dedicated to the Ikea Family Members from Romania, accessible only to the latter, for approximately 40 hours with a number of 114 persons being affected (half of them children).

In this context, the Data Protection Authority highlighted that, according to Recitals 38 of the GDPR, "Children deserve specific protection regarding their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using

services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child".

1.3 ANSPDCP. VODAFONE S.A. was sanctioned for violating the provisions of Article 32 para. (1) lit. b) and para. (4) of the General Data Protection Regulation with a fine in the amount of LEI 7,421.25 (the equivalent of EUR 1,500)

The investigation was initiated as a result of several notifications of personal data breaches transmitted by the controller, based on the provisions of the GDPR and the Regulation (EU) No 611/2013 of 24 June 2013 (on the measures applicable to the notification of personal data breaches).

Regarding to security breaches notified under the GDPR, the Data Protection Authority found that the controller did not implement appropriate technical and organizational measures to ensure that any person acting under the authority of the controller or of the processor and who has access to personal data, will not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

The security breaches led to unauthorized disclosure and/or unauthorized access to personal data of a number of 6 targeted persons.

1.4 ANSPDCP. VALORIS CENTER S.R.L was sanctioned for violating the provisions of Article 29 and Article 32 para. (1) lit. b) and para. (4) of the GDPR with a fine in the amount of LEI 9,898.00 (the equivalent of EUR 2,000)

As a result of the investigation, it turned out that the breach of security occurred due to the fact that a call center employee of the processor, Valoris Center S.R.L., has provided, out of an error, to a controller's customer, an excel file containing the data of the customers of the respective controller that have the Internet Banking service.

The investigation found that the processor, Valoris Center S.R.L., did not implement appropriate measures to ensure that any person acting under his authority and who has access to personal data, will not process those data except on his instructions, which led to unauthorized disclosure and/or unauthorized access to personal data, such as: e-mail, username, user's personal identification number, telephone number, customer's name, customer's code and PIN number) of a number of 11,169 targeted persons.

The investigation was initiated as a result of a notification of personal data breach that was transmitted by a controller, based on the provisions of Article 33 of the GDPR.

II. EUROPEAN UNION

1. REGULATIONS

1.1 EDPB issues guidance on international transfers

At the Plenary Session of the European Data Protection Board, held on November 19, 2021, was adopted the Guidelines no. 05/2021 on the interplay between Article 3 of the GDPR and the provisions on international data transfers under Chapter V of the GDPR.

The Guidelines aim to assist organizations subject to the GDPR in identifying whether a data processing activity constitutes an international data transfer under the GDPR, as the GDPR does not define the term, setting forth three main criteria to be considered in determining whether a processing activity qualifies as an international data transfer under the GDPR, namely:

- The data exporter (controller or processor) is subject to the GDPR for the given processing activity;
- The data exporter discloses by transmission or otherwise makes the personal data subject to the processing of an importer (a controller or processor);
- The data importer is in a third country (or is an international organization), irrespective of whether the data importer or its processing activities are subject to the GDPR in respect of the given processing in accordance with Article 3.

The EDPB welcomes comments on the draft Guidelines by January 31, 2022. The public consultation is available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en).

2. EUROPEAN UNION – SANCTIONS GRANTED IN THE EU

2.1 The Dutch Supervisory Data Protection Authority ("AP") imposed to Transavia airline a fine of EUR 400,000 for breaches of the GDPR provisions

In 2019, the Transavia airline suffered a data breach, in which a hacker gained access to Transavia's systems through two accounts held by the company's IT department. This could have potentially allowed the hacker to access data such as names, dates of birth, gender, email addresses, phone numbers, flight information and booking numbers of 25 million passengers.

Following the investigation, the AP found that the controller had breached its duty to implement technical and organizational measures to ensure a level of security appropriate to the risk to data subjects, which resulted in the unlawful accessing of the personal data of 83,000 targeted persons. In 367 cases, the data included medical information of people who had requested, for example, wheelchair transportation or additional services because they were blind or deaf.

2.2 The Dutch Supervisory Data Protection Authority ("AP") imposed to the Minister of Finance a fine of EUR 2,75 million for breaches of the GDPR provisions

In the context of childcare benefit applications, tax offices had processed data on the dual nationality of applicants for several years. However, the AP found that the data on dual nationality of Dutch citizens would not have been necessary when assessing an application for childcare benefits.

The Minister of Finance pointed out that the personal data had also been processed for the purpose of combating organized fraud and for automatic classification in the authority's risk system.

However, the AP concluded that even for these purposes, the processing would not have been necessary and, for this reason, the tax and customs' administration should have deleted the data on dual nationality as early as January 2014.

Following the investigation, the AP found that the dual citizenship data of a total of 1,4 million people had been unlawfully processed due to the lack of a valid legal basis.

2.3 The Cypriot Data Protection Commissioner ("Cypriot DPC") imposed to WS WiSpear Systems Ltd. a fine of EUR 925,000 for breaches of the GDPR provisions

Following the investigation, the Cypriot DPC found that the controller had collected various data from individuals (Media Access Control addresses and International Mobile Subscriber Identity data) without their knowledge as part of tests and presentations of technologies.

For the non-compliance with general data processing principles and the violation of the principle of legality, objectivity and transparency in the processing of personal data, WS WiSpear Systems Ltd. was sanctioned with a fine of EUR 925,000.