data protection - legal changes published in November 2019

The National Supervisory Authority for Personal Data Processing has sanctioned ING with a fine of 80,000 euros for GDPR violation

Thursday, November 28, 2019, the National Supervisory Authority for the Processing of Personal Data informed that it has completed on November 4, 2019 an investigation at ING Bank N.V. Amsterdam - Bucharest Branch, following a notification, finding that the controller violated the provisions of Article 25 paragraph (1) in conjunction with Article 5 paragraph (1) letter f) from the GDPR, which led to the application of an administrative fine in the amount of 80,000 euros, according to a statement.

In this respect, the controller did not ensure compliance with the principles of privacy by design and privacy by default, because it did not adopt appropriate technical and organizational measures regarding the integration of appropriate safeguards in the automated data processing system during the settlement process of card transactions, affecting a number of 225,525 customers whose payment operations were doubled during the period 08-10.10.2018, also in conjunction to the provisions of Article 32 paragraph (1) letter d) of the GDPR.

Article 5 paragraph (1) letter f) of the GDPR establishes one of the data processing principles, namely that the data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')".

At the same time, according to Article 32 paragraph (1) letter d) of the GDPR, among the appropriate technical and organizational measures that the controller must take in order to ensure a level of security appropriate to the risk, there is the one regarding the existence of a process for periodic testing and assessment of the effectiveness of the technical and organizational measures to guarantee the security of the processing.

The National Supervisory Authority for Personal Data Processing sanctioned TAROM with a fine of 20,000 euros for GDPR violation

On Friday, November 29, 2019, the National Supervisory Authority for Personal Data Processing communicated that it completed on November 7, 2019 an investigation at the controller SC CNTAR TAROM SA and found that it violated the provisions of Article 32 paragraph (4) in conjunction with Article 32 paragraph (1) and paragraph (2) of the GDPR, according to a statement.

The investigation was carried out as a result of the notification of the Supervisory Authority by SC CNTAR TAROM SA on September 13, 2019 regarding a personal data security breach.

The controller SC CNTAR TAROM SA has been sanctioned with an administrative fine of 95,194 lei, the equivalent of 20,000 EURO.

The sanction was applied to the operator due to the fact that it did not implement appropriate technical and organizational measures to ensure that any natural person acting under its authority and having access to personal data, only processes them at its request. Related to this aspect, the controller has not taken any appropriate measures to ensure a level of security corresponding to the risk generated by the unauthorized disclosure or the unauthorized access to the personal data transmitted, stored or otherwise processed.

This situation led to the unauthorized access, by an employee, of the reservation application and the photographing of a list containing the personal data of 22 TAROM passengers/clients and to the unauthorized disclosure of this list online.

The Polish authority imposed a fine of 47,000 Euros for GDPR violation

On Wednesday, November 6, 2019, the President of the Polish Personal Data Protection Office imposed an administrative fine of over PLN 201,000 (approx.. 47,000 EUR) for obstructing the exercise of the right to withdraw consent to the processing of personal data.

The company - ClickQuickNow Sp. z o.o. did not implement appropriate technical and organizational measures that would enable easy and effective withdrawal of consent to the processing of personal data and the exercise of the right to obtain the erasure of personal data (the "right to be forgotten"). Thus, it violated the principles of lawfulness, fairness and transparency of processing of personal data, specified in the GDPR

In his decision, the authority also pointed out that the company processed, without any legal basis, the data of data subjects, who are not its customers and from whom the company received objections to processing their personal data.

The National Supervisory Authority for Personal Data Processing sanctioned Vodafone with a fine of 10,000 lei for GDPR violation

On Wednesday, November 13, 2019, the National Supervisory Authority for Personal Data Processing reported that on October 15, 2019, an investigation was completed at the operator of Vodafone Romania S.A. and found the violation of the provisions of Article 13 paragraph (1) letter q) of Law no. 506/2004, corroborated with Article 13 paragraph (5) of Law no. 506/2004 and with Article 8 of OG 2/2001, according to a statement.

The controller Vodafone România S.A. was given an administrative fine of 10.000 lei.

The sanction was applied because the controller did not consider the option of a claimant to no longer receive marketing messages, and any other messages other than those concerning the costs and security of the calls, an

option brought to the attention of the controller. Although after his request he received a confirmation of being unsubscribed from the marketing communications sent by the controller, he received on his e-mail address another unsolicited message from Vodafone Romania S.A., thus violating the provisions of Article 12 paragraph (1) of Law no. 506/2004 regarding unsolicited communications.

In this context, the company was advised to observe the request of the claimant not to receive marketing messages or any other messages other than those regarding the costs and security of the calls. At the same time, it was recommended to the controller to take the necessary measures to comply with the provisions of Article 12 of Law no. 506/2004, for the purpose of sending marketing messages through electronic means of communication only with the express prior consent of the recipients.

The start date of the calculation of the deadline for communicating a response to the data access requests under the GDPR

Following the ECJ judgment in Case C-171/03 Maatschap Toeters and M.C. The Verberk Productschap Vee en Vleesof, the UK Authority (ICO) has updated its recommendations on data subjects' requests.

Upon setting the deadline for communicating a response to data access requests, the day on which the data access request is received will be considered "Day 1". Thus, the deadline for responding to a request for access to data received on November 5 is fulfilled on December 4 (and NOT on December 5).

The same reasoning must be applied for the calculation of the response time and regarding the exercise of the other rights by the data subjects, regulated by the GDPR.

Law 190/2018 on implementation measures of Regulation (EU) 2016/679 has been amended

Law 233/2019 amended the provision regarding the non-applicability of the rights of the data subjects, namely that they do not apply if the personal data is processed for scientific or historical research purposes or for *statistical purposes*, to the extent that the rights mentioned in these articles are likely to make it impossible or severely affect the achievement of the specific purposes, and the respective derogations are necessary for the fulfillment of these purposes.

Law no. 233/2019 for amending Article 8 paragraph (1) of Law no. 190/2018 regarding implementation measures for Regulation (EU) 2016 / was published in the Official Gazette, Part I no. 956 of November 28, 2019 and entered into force on the date of publication.

Between 12-13 November 2019, the fifteenth Plenary of the European Data Protection Board took place.

The following topics were discussed in the Plenary:

- Guidelines 3/2018 on the territorial scope of the GDPR (art. 3) - final form, after public consultation

  The Committee adopted the final form of the guidelines intended to clarify the applicability of Article 3 of the General Regulation on Data Protection (GDPR), taking into account the feedback received during the public consultation stage. This instrument contains many examples, being intended to ensure a uniform interpretation and application of the provisions of Article 3 of the GDPR at the level of all Member States, in various situations.

- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – under public consultation

  The guidelines contain important aspects regarding the effective interpretation and application of the principles of privacy by design and by default, highlighting the controllers' obligations to take the appropriate technical and organizational measures to ensure the effective observance of the principles of personal data processing and the rights of the data subjects. Also, this document presents operational examples in the specific context of certain processing.

This Guide is under public consultation for 8 weeks, during which proposals and feedback can be submitted.

The third EU-US Privacy Shield Assessment (Privacy Shield) Report was also approved.

The National Supervisory Authority for Personal Data Processing has sanctioned BNP Paribas Personal Finance SA (CETELEM IFN S.A.) with a fine of 9508 Lei for GDPR violation

On Friday, November 22, 2019, the National Supervisory Authority informed that it has completed an investigation at the controller BNP Paribas Personal Finance SA Paris Bucharest Branch (CETELEM IFN S.A.), finding the violation of the provisions of Article 12 paragraph (3) of the GDPR, according to a statement.

The controller BNP Paribas Personal Finance SA was given an administrative fine of 9508 lei, the equivalent of 2000 EURO.

The investigation was initiated as a result of complaints alleging that the controller did not respond to the requester within the time limit provided by Article 12 paragraph (3) of the GDPR, although it had requested the deletion of certain personal data reported in the credit bureau's records system.

According to Article 12 paragraph (3) of the GDPR, the controller has the obligation to respond to the requests of the data subjects without unjustified delays and at the latest within one month from the receipt of the request.

Also, a corrective measure was applied to the controller BNP Paribas Personal Finance SA, which consisted in the adoption of measures, at the company level, regarding the resolution of requests from data subjects, so that, in all cases, the provisions of Article 12 of Regulation (EU) 2016/679 be observed.

The National Supervisory Authority for the Processing of Personal Data has sanctioned FAN COURIER with a fine of 11,000 Euro for violating the provisions of the GDPR

On Monday, November 25, 2019, the National Supervisory Authority for Personal Data Processing informed that, on October 28, 2019, it finalized an investigation at the controller FAN COURIER EXPRESS SRL and found that it violated the provisions of Article 32 paragraph (1) and paragraph (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (GDPR), according to a statement.

The controller FAN COURIER EXPRESS SRL was given an administrative fine in the amount of 52,325.9 lei, the equivalent of 11,000 EURO.

The sanction was applied to the controller because it did not implement adequate technical and organizational measures to ensure a level of security corresponding to the risk of processing generated, in particular, accidentally or illegally, by the destruction, loss, modification, unauthorized disclosure or unauthorized access to the personal data transmitted, stored or otherwise processed, which led to the loss of personal data (name, surname, card number, security code (CVV), card holder address, personal numeric code, identity card series and number , IBAN account number, approved credit limit, correspondence address) and the unauthorized disclosure/ access of the personal data. 1100 data subjects were affected by the security breach although the controller had the obligation to take the adequate security measures for personal data according to the provisions of Article 5 paragraph (1) letter f) of the GDPR.

National Supervisory Authority for Personal Data Processing sanctioned Royal President with a fine of 2,500 euros for GDPR violation

On Friday, November 29, 2019, the National Supervisory Authority for Personal Data Processing informed that on November 18, 2019, it completed an investigation at the controller Royal President S.R.L., finding the following:

- violation of the provisions of Article 12 paragraph (3) and (4) and Article 15 of the GDPR;
- violation of Article 5 paragraph (1) letter f) and Article 32 paragraph (1) letter b) of Regulation (EU) 679/2016.

The controller Royal President S.R.L. was given a warning for violation of the provisions of Article 15 and Article 12 paragraphs (3) and (4) of Regulation (EU) 679/2016 and a fine in the amount of 11,932.25 lei, the equivalent of 2500 EURO for infringing Article 5 paragraph (1) letter f) and Article 32 paragraph (1) letter b) of Regulation (EU) 679/2016.

The sanctions were applied following a complaint alleging that Royal President S.R.L. refused to solve a request to exercise the right of access provided by Article 15 of the General Data Protection Regulation, as well as the fact that it disclosed personal data without the consent of the data subject.

During the investigation, the controller Royal President S.R.L. could provide evidence for solving the request for the exercise of the right of access within the term provided by Article 12 paragraph (3) of Regulation (EU) 2016/679.

It was also found that the personal data collected through the accommodation card were not processed in a way that would ensure their security, by taking appropriate technical or organizational measures, in order to prevent any unauthorized disclosure by infringing the provisions of Article 5 paragraph (1) letter f), Article 32 paragraph (1) letter b) and of Article 32 paragraph (2) of Regulation (EU) 2016/679.

At the same time, a corrective measure was applied to the controller, which consisted in the elaboration and implementation of an internal procedure regarding the protection of personal data of the beneficiaries of the accommodation services, by reference to the provisions of Article 32 of Regulation (EU) 2016/679.

The Belgian authority issued 2 new fines for GDPR violation

The Belgian data protection authority has applied a fine of 5,000 euros to a mayor and a municipal officer in two separate cases.

These fines were applied after they improperly used personal data to send political advertisements so that the mayor would be re-elected during the 2018 Belgian local elections. For the Belgian Litigation Chamber, the behavior of public officials should be exemplary.

The German authority sanctioned a real estate company for violating the GDPR

On October 30, 2019, the Berlin Commissioner for Data Protection and Freedom of Information issued a fine of approximately EUR 14.5 million against Deutsche Wohnen SE for GDPR violations

During the on-site inspections of June 2017 and March 2019, the Supervisory Authority found that this company used an archiving system to store the personal data of tenants, which did not provide the possibility to remove unnecessary data. Tenants' personal data have been stored without checking whether storage is allowed or necessary. In some of the individual cases examined, personal data of the tenants that were kept for a long period

were identified, although these were no longer necessary to meet the purpose initially set. This discovery targeted the personal and financial information of the tenants, such as income statements, self-disclosure forms, extracts from employment and vocational training contracts, tax data, social insurance and health insurance data, and bank statements.

The Data Protection Commissioner of Berlin recommended an urgent adjustment of the archiving system for the first inspection in 2017. However, in March 2019, more than a year and a half after the first inspection and nine months after the start of the GDPR's applicability, the company has not yet been able to demonstrate database cleanup or legal reasons for continuing storage. The company made only preliminary preparations to remedy the deficiencies.

In addition to sanctioning this structural violation, the Data Protection Commissioner of Berlin imposed fines between 6,000 and 17,000 euros on the company for inadmissible storage of personal data of tenants in 15 individual cases.