VOICU FILIPESCU
Attorneys at Law
News in Laws – Legal Monthly Newsletter
February 2021

data protection - legal changes published in January 2021

I. EUROPEAN UNION – regulations

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

The following documents were mainly adopted during the Plenary of the European Data Protection Committee, held online on 14 January 2021:

- Guidelines 01/2021 on Examples regarding Data Breach Notification;
- Guide on the application of art. 62 GDPR (on joint operations of national supervisory authorities);
- Joint opinion of EDPB and EDPS regarding the implementation of the draft European Commission Decision on the standard contractual clauses between the controller and the processor (reported in art. 28 para. 7 of the GDPR);
- Joint opinion no. 1/2020 of the EDPB and EDPS regarding the standard contractual clauses for transfer to third countries.

In this context, we note that the main documents adopted at the previous Plenary in December consisted of:

- Guidelines 10/2020 on restrictions under Article 23 GDPR - version for public consultation;
- Guide no. 2/2020 regarding the application of art. 46 para. (2) letter a) and art. 46 para. (3) lit. b) regarding the transfer of personal data to public authorities from third countries;
- Guide no. 6/2020 on the interaction between the Second Payment Services Directive and the GDPR.

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

II. EUROPEAN UNION - sanctions

1. The Polish authority fined Smart Cities Euro 3,000 for failure to cooperate with the Authority

The Polish authority imposed a fine of more than EUR 3,000 on Smart Cities in Warsaw for failing to cooperate with the Authority by failing to respond to its letter and providing access to personal data and other information necessary for the performance of its tasks.

2. The Belgian authority imposed to Family Service a fine of EUR 50,000

The Authority imposed a fine of EUROS 50,000 on Family Service, which distributes "pink boxes" well known to future mothers and fathers in Belgium. The authority launched an investigation into the company after a complaint was filed alleging that the company transferred personal data to third parties, including data brokers, without valid consent from the customer and without providing sufficient information.

3. The Italian authority requested Facebook and Instagram information about the processing of personal data on the 2 social networks

The authority is stepping up its efforts to protect children who use social networks, following the case of the 10-year-old girl from Palermo and the limitation of TikTok processing. The investigations were started regarding the processing by Facebook and Instagram.

More importantly, specific information was requested on existing registration mechanisms and age verification methods applied by both social networks to verify compliance with the age threshold for registration. Replies from Facebook are expected within 15 days.

4. The Lower Saxony Authority fined notebooksbilliger.de AG with a fine of EUR 10.4 million for video surveillance of employees

The Data Protection Authority of Lower Saxony imposed ***a fine of EUR 10.4 million against notebooksbilliger.de AG.*** The company used ***video surveillance to monitor its employees for at least two years*** without any legal justification. Some of the areas registered by the illegal rooms included workspaces, sales floors, warehouses and staff rooms.

The company claimed that video cameras were installed to prevent and investigate crimes and to track the flow of goods into warehouses. However, in order to prevent theft, a company must first implement less severe means (e.g., random baggage checks on leaving the company headquarters). In addition, video surveillance can only be used to investigate crimes, if certain persons are reasonably suspected of having committed such offenses. In this case, the company may be allowed to monitor people with cameras for a limited period. However, notebooksbilliger.de did not limit its video surveillance to certain employees or to a certain period. In addition, many of the records were saved for 60 days, which is much longer than necessary.

5. The Danish authority issued a warning to a supermarket using facial recognition technology

The Dutch Data Protection Authority has issued an ***official warning*** to a supermarket for ***the use of facial recognition technology.*** Although facial recognition technology has been disabled since December 2019, the supermarket wanted to restart it.

The supermarket claims to have used facial recognition technology to protect its customers and staff and to prevent shoplifting. The technology was connected to the rooms at the entrance to the store. The technology scanned the faces of everyone who entered the store and compared it to a database of people who were denied access to stores. The faces of the people who had not been banned were erased after a few seconds.

Following media reports, on December 6, 2019, the Authority requested information from the supermarket owner. On December 8, 2019, the supermarket turned off facial recognition technology. However, the owner indicated in the documents provided to the Authority that he wished to restart it but was refused.

6. The Polish authority fined the university for the lack of data breach notifications

The President of the Authority for the Protection of Personal Data imposed ***a fine of more than EUR 5,850*** on the Medical University of Silesia, as there was a breach of data protection at the university, which the controller should notify not only the supervisory authority but also the persons affected. of incident.

The students were identified during the exams held at the end of May 2020 through video conferences. After the examination, ***the records were made available*** not only to the persons examined but also to ***others who had access to the system.*** Furthermore, by using a direct link, any third party could have access to the examination records and the personal data of the examined students were presented during the identification.

7. The Polish authority fined ID Finance Poland a fine of EUR 250,000

The punished company (owner of a loan platform MoneyMan.pl) ***did not respond adequately to the signal about its security gaps.*** He did not check the information quickly enough that his client data was available on one of his servers. Such a notification was not taken seriously, so a few days after the company received the signal, an unauthorized person copied the data and then deleted it from the server. The person requested a ransom for the return of the stolen information. Only then did the company start analyzing the security features on its servers and notified the data breach to the supervisory authority at the same time.

8. The Polish authority fined the insurance company WARTA S.A. with a fine in the amount of 20,000 Euros

The insurance and reinsurance company WARTA S.A. was ***fined EUR 20,000 for failing to notify the Authority of a personal data breach.*** In May 2020, the Authority received information from a third party about the personal data breach which consisted in sending by e-mail an insurance policy by an insurance agent, being a processor for WARTA SA Insurance and Reinsurance Company, to an unauthorized recipient.

The attached document contained personal data, including name, surname, residence addresses, PESEL numbers (personal identification numbers) and information on the object of insurance (car). What is important in this case is that the supervisory authority has been informed of the breach of personal data by an unauthorized recipient who has come into possession of documents not intended for it and the confidentiality of the persons concerned has been infringed.

9. The Polish authority fined Virgin Mobile Polska with a fine of EUR 460,000

The Authority imposed a fine of EUR 460,000 on Virgin Mobile Polska for failure to take appropriate technical and organizational measures to ensure the security of the data processed. The Authority stated that the company violated the principles of confidentiality and accountability of the data specified in the GDPR. Virgin Mobile has not performed periodic and comprehensive tests, measurements and evaluations of the effectiveness of the technical and organizational measures applied to ensure the security of the processed data. Activities in this regard were undertaken only when there were suspicions of vulnerability or in connection with organizational changes. Furthermore, no tests were performed to verify the guarantees related to the transfer of data between applications related to the service of prepaid service buyers. In addition, the vulnerability associated with exchanging data in these systems was used by an unauthorized person to obtain data from some of the company's customers.

In connection with a data breach, as a result of which an unauthorized person obtained data from customers in one of the databases, the Authority carried out the inspection at the company. As a result of the irregularities found, the Authority initiated administrative proceedings culminating in the imposition of a fine.