VOICU FILIPESCU
Attorneys at Law
News in Laws – Legal Monthly Newsletter
February 2020

data protection - legal changes published in January 2020

1 DATA PRIVACY DAY – WHAT TO EXPECT IN 2020?

Data Privacy Day (or Data Protection Day as it is known in Europe) is an international event that occurs every year on 28th January. It is currently observed in the United States, Canada, Israel and 47 European countries. The purpose of Data Privacy Day is to raise awareness and promote privacy and data protection best practices.

The priorities established for 2020 are:

- Increased GDPR enforcement;
- Brexit;
- Marketing technologies (Adtech);
- Biometric data (such as facial recognition);
- Artificial intelligence (AI) and new technologies (for example, a unitary approach to voice assistants offered by big tech companies);
- International data transfer;
- Confidentiality of electronic communications (e-Privacy Regulation, expected to enter into force in 2020)

2 EUROPEAN DATA PROTECTION BOARD – THE 17TH PLENARY SESSION HELD ON JANUARY 28TH AND 29TH 2020

During the plenary, the following main documents were adopted:

- **Guidelines 3/2019 on processing of personal data through video devices**

Following the analysis of the proposals submitted in the public consultation phase***, the guidelines were adopted in their final form***, which is a useful tool in the activity of controllers and processors using video surveillance devices. It mainly addresses issues regarding the legality of the processing, the disclosure of images to third parties, the confidentiality and security of the processing, with many relevant examples.

- **Guidelines on connected vehicles**

This document aims to analyze the processing of personal data in the context where the volume of the data used by vehicles has increased significantly. ***The guidelines are under public consultation.***

- **Opinions regarding the drafts of the accreditation requirements of the certification bodies, subject to analysis by the authorities of the United Kingdom and Luxembourg under art. 43 paragraph (3) of the GDPR**

3 GDPR ENFORCEMENT – NATIONAL AND EUROPEAN DEVELOPMENTS

3.1 Romania. 10,000 EURO fine applied to the controller Entirely Shipping & Trading S.R.L. for violating the conditions of video surveillance of employees

On ***January 16, 2020***, the National Authority for Data Protection in Romania informed that it completed on December 13, 2019 an investigation into the controller Entirely Shipping & Trading S.R.L. Following the investigation, the Authority concluded that the controller violated the provisions of the Regulation by not complying with the provisions of art. 12 and art. 13, art. 6 and art. 7, art. 5 paragraph (1) let. c), art. 9, art. 5 paragraph (1) let. a), b) and e) of Regulation (EU) no. 679/2016.

In this case, the Authority became aware, following a ***complaint***, that Entirely Shipping & Trading S.R.L. installed ***audio-video surveillance cameras in employees' offices, changing rooms and in the cafeteria*** and that, in certain locations (restricted access premises), ***access was fingerprint-based***. It was also claimed that the controller ***used the identity of a former employee in sending work e-mails*** without the latter having been informed in advance.

During the investigation, the Authority found that:

- the controller did not prove a ***supported legitimate interest*** for the ***video surveillance*** system installed at its headquarters, which would prevail over the interests or fundamental rights and freedoms of the data subjects, did not prove having ***consulted the union*** or, as the case may be, the ***representatives of the employees*** before the introduction of the surveillance systems, as well as the fact that other less intrusive forms and ways of achieving the purpose pursued by the employer have not previously proved their effectiveness;
- the controller did not prove the existence of ***adequate data protection policies*** and the implementation of ***adequate technical and organizational measures*** to ensure an adequate level of security for this risk;
- ***processing of the biometric data*** through the access control system was not collected for adequate and relevant purposes, limited to what was needed, in relation to the purposes for which they were processed;
- the controller did not carry out a ***data protection impact assessment***

Thus, the controller was sanctioned with **two warnings** but also received **two fines** in the amount of **10,000 Euro** because it excessively processed the personal data (image) of its employees through video cameras, but also for non-compliance with the provisions regarding the processing of employees' biometric data (fingerprints).

At the same time, a series of **corrective measures** were applied to the controller.

3.2 Italy. 3,000 EURO fine applied to the controller Enel Energie S.A. for the processing of personal data without consent

The National Authority has sanctioned the controller Enel Energie S.A. for violating the provisions of art. 5 paragraph (1) let. d) and paragraph (2) in conjunction with art. 6 and art. 7 and art. 21 paragraph (1) of Regulation (EU) no. 679/2016.

The sanctions were imposed following a ***complaint*** alleging that S.C Enel Energie S.A. ***illegally processed the data of the claimant***, unable to prove his/her consent for ***sending notifications to his/her e-mail address*** and without respecting the principle of accuracy. In addition, the controller did not take the necessary measures to disable the transmission of notifications, although the petitioner exercised his/her right to object on several occasions.

The controller S.C. Enel Energie S.A. was sanctioned with **two fines**, each amounting to 14,334.30 lei, the equivalent of 3000 euros, for violating the provisions of Regulation (EU) no. 679/2016

3.3 UK. GBP 500,000 fine applied to a U.K. retail company for not implementing adequate technical and organizational measures for the protection of personal data.

The U.K. Data Protection Authority (ICO) sanctioned DSG Retail Limited for violating the GDPR provisions regarding ensuring an ***adequate level of security*** of personal data ***by not implementing technical and organizational measures appropriate to the risk***.

The investigation carried out by the ICO took place following the report of the ***security incident*** by the retailer on June 8, 2018, by which it confirmed ***unauthorized access to the personal data found in the point of sales terminals*** ("POS"). In this case, the company's IT systems were affected for a period of 9 months, between July 24, 2017 - April 25, 2018, a fact not discovered until April 5, 2018. The company investigated this security breach and discovered that the IT systems were accessed by an unauthorized person who installed a virus, allowing them to collect financial information from POS terminals for any transaction during that period. The controller classified this incident as a ***cyber-attack*** and confirmed that ***5,646,417 bank cards were the target of the attack***, the unauthorized access targeting financial data (card number, expiry date), as well as non-financial data (name, postal address, telephone number, e-mail address), belonging to approximately ***14 million data subjects***.

When setting the amount of the fine, ICO considered that:

- DSG notified 25 million data subjects potentially affected by e-mail and advertising;
- They established a call center to answer questions;
- They notified the ICO of the incident and cooperated with the authorities in the investigation;
- They made significant investments in data security processes and systems;

- They did not detect the breach of by themselves;
- DSG had previously been sanctioned for similar vulnerabilities

The fine is significant but DSG could be forced to also pay damages to the affected persons, which will increase the impact of this incident.

3.4 Cyprus. EUR 82,000 fine for LGS Handling Ltd, Louis Travel Ltd and Louis Aviation Ltd (Louis Group of Companies) for insufficient legal basis for data processing

On Monday***, January 27, 2020***, the Cyprus Authority imposed a fine of € 82,000 on controllers LGS Handling Ltd, Louis Travel Ltd and Louis Aviation Ltd following a ***complaint*** filed by the employees' union.

Following the investigation, it was discovered that the group of companies used the "Bradford Factor" tool to keep track of employees' medical leave. The Authority has found that ***the period and frequency of a person's medical leave***, regardless of whether their identity is directly or indirectly disclosed, ***involves the processing of "special categories of personal data"***, as defined in Article 9 (1) of the General Regulation on Protection data. Thus, the use of such an instrument must be in accordance with the standards set by the GDPR.

In this case, the Authority has established that such a processing operation has no legal basis and has prohibited the further processing of this data, as well as the deletion of the data accumulated until the investigation is completed.

The sanctions were applied as a result of the violation of the provisions of art. 6 paragraph (1) and art. 9 of the GDPR, according to a statement.

3.5 Greece. EUR 15,000 fine for ALLSEAS MARINE S.A for non-observance of employees' right of access to personal data and illegal use of video surveillance systems

On Tuesday, ***January 14, 2020***, the Greek Authority applied a fine of 82,000 Euros to the controller ALLSEAS MARINE SA following the investigation regarding both the legality of the processing of personal data stored on the company server and the employee's right of access to personal data stored in the computer used for the exercise of their profession.

The authority found that the controller ***did not take appropriate measures to allow employees to exercise their right of access*** to personal data, but also that ***the closed-circuit video surveillance system was illegally installed and operated***, and the recorded content presented to the authority was considered illegal.

As a result of the findings, the Authority decided to sanction the controller with ***a fine of 15,000 Euros*** and, at the same time, ordered the company to take measures regarding the compliance with the employees' right of access to personal data, and the use of video surveillance systems to be carried out in accordance with the provisions of the Regulation. The Authority also ordered the controller to review the implementation of the provisions of art. 5 paragraph (1) and (2) GDPR for compliance.