STATE DATA PROTECTION INSPECTORATE

The Fine Issued for Infringements of the GDPR in Mobile Application "Karantinas"
(public sector, 12 thous. Eur; private sector, 3 thous. Eur)

Year 2021

Following the temporary suspension of the use of application "Karantinas" in May 2020 and after an investigation conducted by State Data Protection Inspectorate (DPA) in February 2021, fines for infringements of the General Data Protection Regulation (GDPR) were imposed on the National Public Health Centre (NPHC) and the developer of the application UAB "IT sprendimai sėkmei" (the Company).

A fine of EUR 12,000 was imposed on the NHPC for infringements of provisions of Articles 5, 13, 24, 32, 35 and Article 58(2)(f) of the GDPR, and a fine of EUR 3,000 was imposed on the Company for infringements of Articles 5, 13, 24, 32 and 35 of the GDPR.

In spring 2020, the DPA started monitoring activities in response to information in the media about the possible improper processing of personal data by application "Karantinas". After an assessment of the initial information, it was decided to open an investigation and suspend the processing of personal data by the application.

The study revealed that data from 677 individuals had been collected since April 2020 when the application became operational. Not all personal data were collected to the same extent, however the application was provided for processing such personal data as identification number, latitude and longitude coordinates, country, city, municipality, postal code, street name, house number, name, surname, personal number, telephone number, address, 2nd address, and whether the place of residence had been declared in Lithuania and other information. According to the submitted data, it was established that the processing of data of the app was performed not only in the territory of Lithuania, but also in Europe (Estonia, Switzerland, etc.) and abroad (India, USA, etc.).

After conducting an investigation, the DPA revealed that both the NHPC and the Company were joint data controllers, although both organizations denied such status.

When deciding on the imposition of the administrative fine and its amount, the DPA took into account the fact that the NHPC and the Company processed personal data intentionally, to a large extent, illegally, systematically, without providing technical and organizational means to demonstrate compliance with the requirements of the GDPR while processing personal data, and also processed special category personal data. In addition, the Company did not comply with the DPA instructions to stop the processing of personal data collected with the help of the app and deleted part of the personal data.

The decision of the DPA may be appealed in court within one month from the date of its service in accordance with the procedure established by legal acts.

Additional information on the investigation

Data Protection Impact Assessment (DPIA). The DPA's investigation revealed that a data protection impact assessment (DPIA) was necessary to process the data. Article 35(1) of the GDPR provides that where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The processing of personal data by means of the app should be considered as processing using a new technology and as systematic monitoring, as in this case, the processing was carried out by data subjects using the app for the purpose of self-isolation monitoring and control. It was also intended to process a large number of personal data of data subjects within and outside the territory of Lithuania by means of the app. Moreover, according to the information collected during the DPA's investigation, the processing of personal data was intended to be carried out on a continuous basis. Personal data, including but not limited to, health data of persons identified as vulnerable, namely patients, children, the elderly, etc. were also processed.

Among other things, according to the DPA, the NHPC also managed state information resources by performing the function of prevention and control of communicable diseases and processing personal data collected by the app, whereas the development and management of state information resources not described in the regulations of the state information system breached the requirements of Article 24 and 32 of the GDPR on the implementation of appropriate organisational measures and the principle of integrity and confidentiality provided for in Article 5(1)(f) of the GDPR (personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures).

Violated principles. Considering that the NHPC and the Company failed to prove the lawfulness of the processing of personal data carried out by the app, the DPA found a violation of the principle of lawfulness provided for in Article 5(1) of the GDPR. As neither the NHPC nor the Company acknowledged that they were data controllers at the time of the inspection, both denied their liability as data controllers and accordingly failed to implement the principle of accountability enshrined in Article 5(2) of the GDPR. The principle of transparency was also violated by providing incorrect information about data controllers and processors in the app's privacy policy.

Non-compliance with the instructions. During the DPA's verification of the personal data processed by the app, it was important to assess the true scope and nature of the personal data processing, therefore, the DPA instructed the Company to suspend the processing of personal data by the app, but the Company deleted the data. By deleting the personal data processed by the app, the Company failed to properly implement the instructions given to it by the DPA, and violated Article 58(2)(f) of the GDPR. It should be noted that such failure to comply with the instructions of the DPA entails liability to the Company provided for in Article 83(5)(e) of the GDPR.