July 21, 2022

Administrative fine of HRK 2.15 million due to failure to take appropriate technical and organizational measures

The Personal Data Protection Agency imposed an administrative fine in the amount of HRK 2.15 million on the data controller - telecommunications service provider for failing to take appropriate technical and organizational security measures for the processing of personal data, which led to the unauthorized processing of the personal data of approximately 100,000 respondents, i.e. unauthorized access to personal data by attackers. The controller did not take the necessary measures to achieve an adequate security measure in accordance with the existing foreseeable risks, thereby acting contrary to Article 25 paragraph 1 and Article 32 paragraph 1 points b) and d) and paragraph 2 of the General Data Protection Regulation.

The Agency learned about the violation in question from the data controller through the received Report on the violation of personal data, in accordance with Article 33, paragraph 1 of the General Regulation on Data Protection. Also, the data controller informed the users of its services about the incident in question.

In the case in question, it was established that the data controller implements certain organizational and technical measures when processing personal data, but in the specific case they were not sufficient. Namely, the processing manager made multiple omissions during the design of the processing system, including limiting access, monitoring, reporting, timely response and inclusion of appropriate corrective actions in the system, and execution of the prescribed organizational measures contained in the existing internal acts and, finally, their changes in accordance with the provisions in the relevant hurt. For the aforementioned violations, the General Data Protection Regulation stipulates the imposition of an administrative fine in accordance with Article 83, paragraph 4, point a), that is, an administrative fine of up to EUR 10,000,000 or, in the case of an entrepreneur, up to 2% of the total annual turnover at the world level for the previous financial year, whichever is greater.

Likewise, the Agency finds as an aggravating circumstance the fact that the data controller is one of the leading companies providing telecommunications services in the Republic of Croatia, and it was to be expected that due to the large volume of personal data it processes, it will apply more complex organizational and technical protection measures before the start, as well as during the processing itself, taking into account the latest achievements, the cost of implementation and the nature, scope, context and purposes of processing, as well as risks of different levels of probability and severity for the rights and freedoms of individuals arising from data processing, and especially after the breach in question, which is the same society failed to do.

Following the established circumstances, the Agency, in accordance with its powers from Article 58, paragraph 2, point of the General Data Protection Regulation, imposed an administrative fine, all in accordance with the conditions for its imposition from Article 83 of the General Regulation and Articles 44, 45 and 46 of the Act on the Implementation of the General Regulation on Data Protection.

Administrative fine of HRK 30,000 for not marking the facility under video surveillance

The Agency for the Protection of Personal Data ex officio, without prior notice, carried out direct supervision over the processing and enforcement of personal data protection, collection and processing of personal data made by the video surveillance system, and determined that the processing manager - the car sales and service center based in Zagreb was not indicated that certain rooms in it, as well as the external surfaces of the object in question, are under video surveillance, which is against Article 27, Paragraph 1 of the Law on the Implementation of the General Regulation on Data Protection.

In accordance with Article 51, paragraph 1, subparagraph 1 of the Act on the Implementation of the General Regulation on Data Protection, the Agency imposed an administrative fine in the amount of HRK 30,000 for the aforementioned violation.

Precisely the corrective measure in the form of an administrative fine is effective, proportional and deterrent and fully appropriate to the circumstances for both imposed fines, which are paid to the state budget.