The Agency for the Protection of Personal Data imposed an administrative fine on the data controller - a trading company for organizing games of chance - betting games (sports bookmaker) in the amount of 380,000.00 euros due to the following violations of the General Data Protection Regulation:

The data controller processed personal data, i.e. copies of bank cards of the respondents, for which no legal basis was proven, which violated Article 6, paragraph 1 of the General Regulation on Data Protection;

The data controller did not adequately inform the respondents about the processing of personal data, that is, about the processing of data contained on copies of bank cards, which violated Article 13, paragraphs 1 and 2 of the General Data Protection Regulation;

When creating a new business process for a quick payment service to a VISA bank card, the data controller did not implement appropriate technical and organizational measures, thereby violating Article 25, paragraph 1 and 2 of the General Data Protection Regulation;

The controller did not apply a technical encryption measure to the personal data of the respondents stored in the controller's databases and did not regularly assess the effectiveness of technical and organizational measures to ensure the security of the processing, which violated Article 32, paragraph 1, point a) and d) of the General Protection Regulation data.

Namely, the Agency received a citizen's submission about the collection of a two-sided copy of the bank card via electronic mail by the processing manager in question. Pursuant to the authority, the Agency initiated the procedure ex officio due to the high risk to the rights and freedoms of the respondents (players, users of the service).

In the case in question, it was determined that from June to December 2022, the processing manager provided players with an additional service of paying out winners to a VISA card, in addition to the already existing options for paying out funds from the user's account to a bank account. It was determined that the processing or collection of copies of bank cards is not necessary in order to comply with the legal obligations arising from the Law on Prevention of Money Laundering, since the in-depth analysis of players can be carried out without collecting copies of both sides of bank cards. As a result of the above, the processing manager illegally processed copies of bank cards using inadequate means of processing and stored them without applying appropriate technical and organizational measures.

Also, the data controller did not inform the respondents about the processing in question (storage of copies of bank cards) in accordance with the principle of transparency, and thus the respondents were deprived of basic information about data

processing such as the legal basis, purpose and storage period. Namely, in the Statement on personal data protection measures, which forms part of the Privacy Policy, it was expressly stated that the data controller does not store bank card numbers and that the numbers are not accessible to unauthorized persons.

However, employees of the processing manager in the period June - December 2022 had access to 655 copies of bank cards on which the full extent of data was visible out of a total of 2078 copies of bank cards collected. Such processing resulted in a high-risk violation of a third of the total processed data, and the respondents were not even aware that this data was stored in databases.

Given that financial data is considered a sensitive category of personal data, which depending on the context and scope of processing can cause a high risk for the rights and freedoms of the data subject, the controller was obliged to pay special attention to the security and legality of the processing, which was taken taken into account as an aggravating circumstance.

As a mitigating circumstance in the specific procedure, the degree of responsibility shown by the data controller after the supervision was carried out - he informed the Agency on his own initiative about the way in which he plans to harmonize the processing with the provisions of the General Data Protection Regulation. Thus, the processing manager made additional investments in payment processes in such a way that the system was improved and that the delivery of a copy of the bank card is no longer requested, and all stored copies of the bank cards were deleted. Also, the processing manager stated that he improved the business processes of monitoring the processing of personal data and educated employees.