https://uodo.gov.pl/pl/138/3854

26/08/2025

The bank cannot scan customers' ID cards without appropriate analysis of the purpose.

The processing of personal data obtained by copying (scanning) identity documents by a bank must be preceded by a justification analysis, i.e., verifying whether such an action is truly necessary. The bank failed to do so and excessively scanned the identity cards of customers and potential customers, even when they filed complaints, for example. Hence the fine imposed by the President of the Personal Data Protection Office, Mirosław Wróblewski, in the amount of PLN 18,416,400.

From April 1, 2019, to September 23, 2020, ING Bank Śląski scanned the identity documents of clients and potential clients. No verification was made as to whether such activities were justified by the bank's requirement to apply financial security measures under the Anti-Money Laundering and Counter-Terrorism Financing (AML) Act.

The Personal Data Protection Office conducted an inspection of the bank's processing of personal data from its customers and potential customers. The inspection involved copies (scans) of identity documents. The inspection examined, in particular, the legal basis for personal data processing, the scope and type of personal data processed, and the method and purpose of data collection and sharing.

It turned out that before the amendment to the AML Act on July 13, 2018, the bank had not been copying customer ID documents. However, after conducting analyses, reconciliations, and implementing changes to banking processes, a change in practice and procedures occurred. It was assumed that in each of the cases indicated in these procedures and instructions, a scan of the customer's or potential customer's ID document should be performed – in many situations, obtaining this document was a condition for performing any activities on behalf of the customer.

Therefore, the bank did not conduct an individual risk assessment of a given client and their actions . Identity documents were also scanned in cases not related to fulfilling obligations specified in the AML Act (e.g., during a complaint regarding an ATM).

Scanning of identity cards by obligated institutions is legal in the context of the AML Act only if it is related to the application of financial security measures necessary under this Act to counteract money laundering and terrorism financing.

The bank's task is to conduct an individual assessment of money laundering and terrorism financing risk and design security measures appropriate to its findings (risk-based approach). Only if the obligated institution demonstrates that, to counteract money laundering and terrorism financing, it is necessary to implement financial security measures that involve processing information contained in identity documents and making copies (scans) of them, does it have the right to demand their implementation.

The Bank, as a data controller, through its actions violated personal data protection regulations (Article 5(1)(a), (b), and (c), as well as Article 6(1) of the GDPR). The violation consisted of the unjustified processing of personal data of current and potential customers obtained through the scanning of identity documents in situations unrelated to its obligations under the AML Act.

According to the bank's reports, for example, in 2020, the number of customers was 4.72 million, including 4.24 million individual customers and 486,000 corporate customers. Mass processing must be associated with a higher level of responsibility on the part of the controller and a higher level of due diligence required of it, as it may result in negative consequences for many individuals.

https://uodo.gov.pl/pl/138/3854

It should also be noted that the Bank should be expected to take a professional approach to the legal basis for data processing.

The Bank's explanations indicate that the practice of copying identity documents concerned a potentially large group of customers over a relatively long period of time (i.e. for a period of approximately 18 months: from 1 April 2019 to 23 September 2020), which indicates the large scale of this processing, but no customers were found to have suffered any damage as a result.

The personal data processed by the Bank, obtained by scanning identity documents, do not fall within the special categories of personal data referred to in Article 9(1) and Article 10 of the GDPR, however their scope (i.e., among others: first name and last name, PESEL number, image, date of birth, parents' names, maiden name, number and series of the identity document) is associated with a high risk of violating the rights and freedoms of natural persons.

The PESEL number together with the name and surname uniquely identifies a natural person, in a way that allows the negative consequences of a violation (e.g. identity theft, loan fraud) to be attributed to that specific person.

In the opinion of the President of the Personal Data Protection Office, the administrative fine applied in this individual case is effective, proportionate and dissuasive.

DKN.5112.6.2020