

Brak zgłoszenia naruszenia ochrony danych, a kara dla Administratora

W ostatnim czasie miało miejsce upublicznienie dokumentów bankowych, znajdujących się w porzuconej na jednym z osiedli przesyłce, po tym jak została ona wcześniej skradziona firmie kurierskiej. W przesyłce były m.in. takie dane jak: imiona i nazwiska, daty urodzenia, numery rachunków bankowych, dane adresowe i kontaktowe, numery PESEL, nazwy użytkowników i hasła do banku, czy dane o zarobkach, seria i numery dowodu osobistego, informacje o produktach bankowych.

Bank tłumaczył, że nie zgłosił tego naruszenia, gdyż przesyłka została odnaleziona przez jedną zidentyfikowaną osobę w krótkim czasie, po jej utracie przez kuriera. Ponadto ustalono, że nie brakowało w niej żadnych dokumentów, a osoba, która znalazła dokumenty, zaniósła je bezpośrednio na posterunek policji i oświadczyła, że nie kopiowała znalezionych dokumentów.

W przypadku wystąpienia naruszenia ochrony danych, oceny ryzyka naruszenia praw lub wolności osoby fizycznej powinno się dokonać przez pryzmat osoby zagrożonej, a nie interesów administratora. Zaznaczył przy tym, że brak zawiadomienia o naruszeniu ochrony danych osobowych osób dotkniętych tym naruszeniem, w przypadku wystąpienia wysokiego ryzyka naruszenia ich praw lub wolności, pozbawia je nie tylko możliwości odpowiedniej reakcji na naruszenie, ale również możliwości dokonania samodzielnej oceny naruszenia, które może powodować dla nich poważne konsekwencje. Brak zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO pozbawia z kolei organ nadzorczy możliwości odpowiedniej reakcji na naruszenie, a więc oceny ryzyka naruszenia dla praw lub wolności osoby fizycznej, ale również szansy na weryfikację, czy administrator zastosował właściwe środki w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą. Organ nie jest wówczas w stanie ocenić czy administrator zastosował odpowiednie środki bezpieczeństwa w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia.

Przy ustalaniu wymiaru kar UODO wskazał, że jest to kolejne naruszenie ochrony danych osobowych, które zostało stwierdzone u tego administratora, wobec czego nałożył na Santander Bank Polska S.A. administracyjną karę pieniężną w wysokości 545 tys. zł.

Prezes UODO ukarał także Toyota Bank Polska S.A. W tym przypadku kara wyniosła 78 tys. zł i została nałożona za niezgłoszenie Prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Administrator zgłosił naruszenie ochrony danych półtora roku po jego wystąpieniu, w momencie gdy zwrócił się do niego organ nadzorczy po otrzymaniu skargi od osoby poszkodowanej tym naruszeniem.

Pełna treść artykułu UODO oraz decyzji znajduje się pod poniższym linkiem:

<https://uodo.gov.pl/pl/138/3049>