ODPIS

106

Sygn. akt II SA/Wa 4143/21

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 1 lipca 2022 r.

Wojewódzki Sąd Administracyjny w Warszawie
w składzie następującym:

Przewodniczący Sędzia WSA	Joanna Kruszewska-Grońska
Sędzia WSA	Joanna Kube (spr.)
Sędzia WSA	Waldemar Śledzik
Protokolant referent stażysta	Beata Kowalska

po rozpoznaniu na rozprawie w dniu 21 czerwca 2022 r.
sprawy ze skargi Banku Millenium S.A. z siedzibą w Warszawie
na decyzję Prezesa Urzędu Ochrony Danych Osobowych
z dnia 14 października 2021 r. nr DKN.5131.16.2021
w przedmiocie przetwarzania danych osobowych

oddala skargę

WOJEWÓDZKI SĄD ADMINISTRACYJNY W WARSZAWIE

Na oryginale właściwe podpisy
Za zgodność z oryginałem

Marcin Rusinowicz-Borkowski

sekretarz sądowy

UZASADNIENIE

Prezes Urzędu Ochrony Danych Osobowych (dalej: „organ", „Prezes UODO") decyzją z dnia 14 października 2021 r., na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2021 poz. 735 z późn. zm.), dalej: „k.p.a.", art. 7 ust. 1 oraz art. 60, art. 101 i art. 103 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), a także art. 57 ust. 1 lit. a) i h), art. 58 ust. 2 lit. e) oraz i), art. 83 ust. 1 i ust. 2, art. 83 ust. 4 lit. a) w związku z art. 33 ust. 1 oraz art. 34 ust. 1, 2 i 4 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35), dalej: „RODO", po przeprowadzeniu postępowania administracyjnego wszczętego z urzędu w sprawie braku zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO oraz braku zawiadomienia o naruszeniu ochrony danych osobowych osób, których dotyczyło naruszenie, przez Bank Millennium S.A. z siedzibą w Warszawie, dalej: „Bank", Prezes UODO

1) stwierdzając naruszenie przez Bank przepisów:

a) art. 33 ust. 1 RODO, polegające na niezgłoszeniu Prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia oraz

b) art. 34 ust. 1 RODO, polegające na niezawiadomieniu o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki osób, których dane dotyczą,

nałożył na Bank administracyjną karę pieniężną w wysokości 363.832 PLN (słownie: trzysta sześćdziesiąt trzy tysiące osiemset trzydzieści dwa złote),

2) nakazał Bankowi zawiadomienie - w terminie 3 dni od dnia doręczenia niniejszej decyzji - oraz , dalej: „skarżący", o naruszeniu ochrony ich danych osobowych w celu przekazania im informacji wymaganych zgodnie z art. 34 ust. 2 RODO, tj.:

a) opisu charakteru naruszenia ochrony danych osobowych;

b) imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisu możliwych konsekwencji naruszenia ochrony danych osobowych;
d) opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jak wynika z ustaleń organu, w dniu kwietnia 2019 r. Oddział Banku nadał do Centrali Banku przesyłkę, w której znajdowały się następujące dokumenty: pełnomocnictwo udzielone skarżącemu przez skarżącą, umowa konta oszczędnościowego profit, umowa rachunków bankowych oraz karty debetowej, umowa ramowa o świadczenie usług finansowych, umowa rachunku bankowego, potwierdzenie zmian do umowy rachunku bankowego, umowa karty Millennium Visa Prestige, ankieta inwestycyjna, wynik ankiety inwestycyjnej. Na ww. dokumentach znajdowały się w szczególności następujące dane: imię, nazwisko, PESEL, adres zameldowania, numery rachunków bankowych, numer CIF (numer identyfikacyjny nadawany klientom Banku) skarżącej oraz imię, nazwisko i PESEL skarżącego. Przesyłka zawierająca ww. dokumenty powinna dotrzeć do Centrali Banku w dniu kwietnia 2019 r. W dniu kwietnia 2019 r. Bank podjął działania w celu wyjaśnienia z firmą kurierską DPD Polska Sp. z o.o. z siedzibą w Warszawie, dalej: „DPD", opóźnienia w doręczeniu ww. przesyłki. Następnie, w dniu kwietnia 2019 r. Bank złożył oficjalną reklamację w związku z brakiem doręczenia ww. przesyłki. W dniu ‹wietnia 2019 r. firma kurierska poinformowała Bank o zmianie statusu ww. przesyłki na status zagubionej informując, że pomimo tego nadal podejmuje próby wyjaśnienia sprawy. W dniu maja 2019 r. firma kurierska poinformowała Bank, że nie zdołała zlokalizować przesyłki i zakończyła próby jej poszukiwania.

Bank, zgodnie z metodyką opartą na europejskiej metodologii ENISA, ocenił to zdarzenie, jako mogące powodować średnie ryzyko naruszenia praw i wolności skarżących.

Bank nie zgłosił ww. naruszenia do Prezesa UODO oraz nie zawiadomił osób o naruszeniu ochrony ich danych osobowych w trybie art. 34 ust. 1 RODO, wskazując im w przesłanej informacji o zagubionych dokumentach ogólne informacje dotyczące charakteru naruszenia oraz środki w celu zminimalizowania jego ewentualnych negatywnych skutków, w tym umożliwiając skarżącym skorzystanie z bezpłatnej usługi Alert BIK.

Organ w związku z brakiem zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO oraz brakiem zawiadomienia o naruszeniu ochrony

danych osobowych osób, których dotyczyło naruszenie przeprowadził z urzędu postępowanie administracyjne, w wyniku czego wydał wskazaną na wstępie decyzję z dnia 14 października 2021 r., w której zważył co następuje:

Zgodnie z art. 4 pkt 12 RODO naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Art. 33 ust. 1 i 3 RODO zaś stanowi, że w przypadku naruszenia ochrony danych osobowych, administrator danych bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia (ust. 1). Zgłoszenie, o którym mowa w ust. 1 musi, co najmniej: a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych; d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków (ust. 3).

Z kolei art. 34 ust. 1 RODO wskazuje, że w sytuacji możliwości wystąpienia wysokiego ryzyka dla praw i wolności osób fizycznych wynikających z naruszenia ochrony danych osobowych, administrator jest zobowiązany bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, o naruszeniu. Zgodnie z art. 34 ust. 2 RODO, prawidłowe zawiadomienie powinno:

1) jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych;

2) zawierać przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO, tj.:

a) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji;
b) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
c) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Organ stwierdził, że zgłaszanie naruszeń ochrony danych osobowych przez administratorów stanowi skuteczne narzędzie przyczyniające się do realnej poprawy bezpieczeństwa przetwarzania danych osobowych. Zgłaszając naruszenie organowi nadzorczemu, administratorzy informują Prezesa UODO, czy w ich ocenie wystąpiło wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą oraz - jeśli takie ryzyko wystąpiło - to czy przekazali stosowne informacje osobom fizycznym, na które naruszenie wywiera wpływ. W uzasadnionych przypadkach mogą również przekazać informację, że powiadomienie w ich ocenie nie jest konieczne ze względu na spełnienie warunków określonych w art. 34 ust. 3 lit. a) i b) RODO. Prezes UODO dokonuje weryfikacji oceny dokonanej przez administratora i może - jeżeli administrator nie zawiadomił osób, których dane dotyczą - zażądać od niego takiego zawiadomienia.

Zgłoszenia naruszenia ochrony danych osobowych pozwalają organowi nadzorczemu na właściwą reakcję mogącą ograniczyć skutki takich naruszeń, bowiem administrator ma obowiązek podjęcia skutecznych działań zapewniających ochronę osobom fizycznym i ich danym osobowym, które z jednej strony pozwolą na kontrolę skuteczności dotychczasowych rozwiązań, a z drugiej ocenę modyfikacji i usprawnień służących zapobieżeniu nieprawidłowościom analogicznym do objętych naruszeniem. Natomiast zawiadomienie osób fizycznych o naruszeniu zapewnia możliwość przekazania tym osobom informacji na temat ryzyka związanego z naruszeniem oraz wskazania działań, jakie osoby te mogą podjąć, aby uchronić się przed potencjalnymi negatywnymi skutkami naruszenia.

Natomiast sama ocena naruszenia przeprowadzona przez administratora pod kątem ryzyka naruszenia praw lub wolności osób fizycznych niezbędna do oceny, czy doszło do naruszenia ochrony danych skutkującego koniecznością zawiadomienia Prezesa UODO (art. 33 ust. 1 i 3 RODO) oraz osób, których dotyczy

naruszenie (art. 34 ust. 1 i 2 RODO), powinna być dokonana przez pryzmat osoby dotkniętej naruszeniem.

Prezes UODO stwierdził, że naruszenie poufności danych, jakie wystąpiło w przedmiotowej sprawie, w związku z naruszeniem ochrony danych osobowych polegającym na zagubieniu dokumentacji zawierającej dane osobowe, klientów Banku w zakresie m.in.; imię, nazwisko, nr PESEL, adres zameldowania, numery rachunków bankowych, numer CIF (numer identyfikacyjny nadawany klientom Banku) skarżącej oraz imię, nazwisko, nr PESEL skarżącego, powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych. To z kolei skutkuje powstaniem po stronie Banku obowiązku zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu zgodnie z art. 33 ust. 1 RODO, w którym muszą się znaleźć informacje określone w art. 33 ust. 3 RODO oraz zawiadomienia tych osób o naruszeniu, zgodnie z art. 34 ust. 1 RODO, w którym muszą się znaleźć informacje określone w art. 34 ust. 2 RODO.

Zaznaczył, że nie jest istotne przy tym to, czy nieuprawniony odbiorca faktycznie wszedł w posiadanie i zapoznał się z danymi osobowymi innych osób, lecz to, że wystąpiło takie ryzyko, a w konsekwencji również potencjalnie wystąpiło ryzyko naruszenia praw lub wolności podmiotów danych, które z uwagi na zakres danych uznał jako wysokie. Zwrócił przy tym uwagę, że choć Bank ocenił, że zaistniałe naruszenie nie wiąże się z ryzykiem naruszenia praw lub wolności osób nim dotkniętych, ponieważ dane nie posłużyły np. do wyłudzenia kredytu ani próby takiego wyłudzenia, utrata przesyłki nie spowodowała też innych niedogodności, to jednak przewidział, że naruszenie to może wiązać się z takim ryzykiem, skoro zaproponował, w ramach środków w celu zaradzenia naruszeniu, dodatkową usługę BIK Alert.

Zdaniem organu, dla powstania obowiązku zawiadomienia o naruszeniu ochrony danych osobowych osób, których dane dotyczą, nie jest konieczne zmaterializowanie się negatywnych konsekwencji naruszenia, wystarczająca jest w tym zakresie sama możliwość (ryzyko) wystąpienia takich konsekwencji, które w niniejszej sprawie, w ocenie organu nadzorczego, jest wysokie.

Art. 34 ust. 1 RODO stanowi, że jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu.

Natomiast art. 33 ust. 1 RODO stanowi, że w przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki, zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Prezes UODO, odwołując się do treści powyższych przepisów stwierdził, że dokonując oceny ryzyka naruszenia praw lub wolności osób fizycznych, od której uzależnione jest dokonanie zgłoszenia naruszenia ochrony danych osobowych oraz zawiadomienie o naruszeniu osoby, której dane dotyczą, należy łącznie uwzględnić czynnik prawdopodobieństwa i wagę potencjalnych negatywnych skutków. Wysoki poziom któregokolwiek z tych czynników ma wpływ na wysokość ogólnej oceny, od której uzależnione jest wypełnienie obowiązków określonych w art. 33 ust. 1 i art. 34 ust. 1 RODO.

Prezes UODO uznał, że ze względu na zakres ujawnionych danych osobowych wystąpiła możliwość zmaterializowania się doniosłych negatywnych konsekwencji dla osób, których dane dotyczą, wagę potencjalnego wpływu na prawa lub wolności osób fizycznych należy uznać za wysoką. Jednocześnie stwierdził, że prawdopodobieństwo wystąpienia wysokiego ryzyka w następstwie niniejszego naruszenia nie jest małe i nie zostało wyeliminowane. Wystąpienie, w związku z przedmiotowym naruszeniem, wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą, determinuje obowiązek dokonania zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienia o naruszeniu tych osób.

Zaznaczył, że brak zgłoszenia przedmiotowego naruszenia ochrony danych osobowych Prezesowi UODO przez Bank jest niezrozumiały w związku z tym, że sam administrator w przeprowadzonej ocenie ryzyka naruszenia praw lub wolności skarżących przyjął średni poziom tego ryzyka. Określone na tym poziomie ryzyko naruszenia praw lub wolności osób fizycznych, nie wyłącza zaś obowiązku, o którym mowa w art. 33 ust. 1 RODO. Bank zatem stosownie do wyniku własnej analizy ryzyka przeprowadzonej w związku z naruszeniem powinien co najmniej dokonać zgłoszenia naruszenia organowi nadzorczemu, czego nie uczynił.

Organ wyjaśnił, że ani na gruncie RODO, ani żadnego innego aktu prawnego, nie funkcjonuje enumeratywne wyliczenie zdarzeń kwalifikowanych jako naruszenie ochrony danych osobowych. Art. 4 pkt 12 RODO stanowi, iż naruszenie ochrony danych osobowych rozumiane jest jako: naruszenie bezpieczeństwa, prowadzące do

przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Zawarte w ww. przepisie wyliczenie operacji przetwarzania posiada charakter wyłącznie przykładowy, w istocie bowiem każda operacja przetwarzania może wiązać się z naruszeniem bezpieczeństwa danych. W przypadku wykrycia przez administratora naruszenia ochrony danych osobowych, w pierwszej kolejności konieczne jest dokonanie analizy pod kątem wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Administrator zwolniony jest z obowiązku powiadamiania organu nadzorczego o naruszeniu, jeśli w wyniku przeprowadzonego badania okaże się, że nie ma prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Należy jednak mieć na względzie fakt, iż organ nadzorczy będzie mógł zwrócić się do administratora o uzasadnienie decyzji o niezgłaszaniu naruszenia, w związku z tym wnioski z przeprowadzonej analizy należy odnotować w wewnętrznej ewidencji naruszeń.

Organ zwrócił uwagę, że w okresie, w którym doszło do naruszenia podobne przypadki były zgłaszane organowi nadzorczemu, a naruszenia z sektora bankowego/ubezpieczeniowego, jak wynika ze Sprawozdania z działalności Prezesa UODO w roku 2019, były jednymi z najczęstszych, jakie wpływały do organu nadzorczego. W zdecydowanej większości dokonywane Prezesowi UODO zgłoszenia naruszenia ochrony danych osobowych dotyczą zagubienia dokumentacji zawierających dane osobowe, głównie w formie papierowej przez operatorów pocztowych lub podmioty świadczące usługi kurierskie, jak ma to miejsce w przedmiotowej sprawie. Wówczas, co również wynika ze Sprawozdania, w ramach działań naprawczych administratorzy dokonywali przeglądu umów zawartych z tymi podmiotami oraz ustalano przyczyny zaistniałych zdarzeń.

Organ zwrócił uwagę na konsekwencje, z jakimi może wiązać się ujawnienie nr PESEL, w tym w szczególności kradzieży tożsamości. Zjawisko kradzieży tożsamości wciąż się nasila, o czym świadczą wpływające nieustannie do Urzędu sygnały od osób poszkodowanych, jak również administratorów zgłaszających naruszenia w tym zakresie.

W ocenie Prezesa UODO, administrator, biorąc pod uwagę charakter naruszenia oraz kategorie danych, które uległy naruszeniu, powinien wskazać

osobom, których dane dotyczą, najbardziej prawdopodobne, negatywne konsekwencje naruszenia ich danych osobowych.

W przypadku naruszenia takich danych, jak imię, nazwisko oraz nr PESEL, możliwa jest kradzież lub sfałszowanie tożsamości poprzez uzyskanie przez osoby trzecie, na szkodę osób, których dane naruszono, pożyczek w instytucjach pozabankowych bądź wyłudzenia ubezpieczenia lub środków z ubezpieczenia, co może spowodować negatywne konsekwencje związane z próbą przypisania osobom, których dane dotyczą, odpowiedzialności za dokonanie takiego oszustwa. Opis możliwych konsekwencji powinien zaś odzwierciedlać ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić jej podjęcie niezbędnych działań zapobiegawczych.

Organ zaznaczył, że Bank w przypadku dołączanych do zgłaszanych naruszeń ochrony danych osobowych (w zakresie ujawnienia nr PESEL) powiadomień kierowanych do osób, których dane dotyczą, każdorazowo wskazuje na konsekwencję w postaci „kradzieży lub sfałszowania tożsamości", niezrozumiałe jest zatem, w ocenie Prezesa UODO, kompletne zmarginalizowanie tego ryzyka w wyjaśnieniach, jakie złożył Bank w toku postępowania.

Zwrócił uwagę, że zgłaszając naruszenie organowi nadzorczemu, administratorzy informują Prezesa UODO, czy w ich ocenie wystąpiło wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą oraz - jeśli takie ryzyko wystąpiło - czy przekazali stosowne informacje osobom fizycznym, na które naruszenie wywiera wpływ. W uzasadnionych przypadkach mogą również przekazać informację, że powiadomienie, w ich ocenie, nie jest konieczne ze względu na spełnienie warunków określonych w art. 34 ust. 3 lit. a) i b) RODO.

Prezes UODO dokonuje weryfikacji oceny dokonanej przez administratora i może - jeżeli administrator nie zawiadomił osoby - zażądać od niego takiego zawiadomienia. W sytuacji braku zgłoszenia naruszenia ochrony danych osobowych Prezes UODO pozbawiony jest możliwości przeprowadzenia rzetelnej weryfikacji. W sytuacji, gdy na skutek naruszenia ochrony danych osobowych występuje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator zobowiązany jest wdrożyć wszelkie odpowiednie środki techniczne i organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy, a w przypadkach wysokiego ryzyka naruszenia praw lub wolności,

również osoby, których dane dotyczą. Administrator powinien zrealizować przedmiotowy obowiązek możliwie najszybciej.

Właściwe wywiązanie się z obowiązku określonego w art. 34 RODO ma zapewnić osobom, których dane dotyczą, szybką i przejrzystą informację o naruszeniu ochrony ich danych osobowych wraz z opisem możliwych konsekwencji naruszenia ochrony danych osobowych oraz środków, które mogą one podjąć w celu zminimalizowania jego ewentualnych negatywnych skutków. Postępując zgodnie z prawem i wykazując dbałość o interesy osób, których dane dotyczą, Bank powinien był bez zbędnej zwłoki zapewnić osobom, których dane dotyczą, możliwość jak najlepszej ochrony danych osobowych. Dla osiągnięcia tego celu niezbędne jest przynajmniej wskazanie tych informacji, które wymienione są w art. 34 ust. 2 RODO, z którego to obowiązku Bank nie wywiązał się. Bank, podejmując zatem decyzję o niezawiadomieniu o naruszeniu organu nadzorczego, jak i osób, których dane dotyczą, w praktyce pozbawił te osoby, przekazanej bez zbędnej zwłoki, rzetelnej informacji o naruszeniu i możliwości przeciwdziałania potencjalnym szkodom.

Przesłana do skarżących przez Bank informacja o zagubionych dokumentach nie zawiera elementów, o których mowa w art. 34 ust. 2 RODO, co oznacza w konsekwencji, że nie może zostać uznana za zawiadomienie o naruszeniu ochrony danych osobowych. Prawidłowe zawiadomienie powinno bowiem jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO. Tymczasem informacja przesłana do skarżących zawierała jedynie bardzo ogólny opis charakteru naruszenia (bez wskazania kategorii danych objętych naruszeniem) oraz środki w celu zminimalizowania jego ewentualnych negatywnych skutków, w tym umożliwienie skorzystania skarżącym z bezpłatnej usługi Alert BIK. W ww. piśmie nie umieszczono natomiast opisu możliwych konsekwencji, z jakimi wiązać się może przedmiotowe naruszenie ochrony danych osobowych oraz informacji o imieniu i nazwisku oraz danych kontaktowych inspektora ochrony danych lub oznaczeniu innego punktu kontaktowego, od którego można uzyskać więcej informacji.

Brak w niej również odniesienia się do środków bezpieczeństwa zastosowanych przez administratora w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia.

Prezes UODO w związku z powyższym stwierdził, że Bank nie dokonał zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu w wykonaniu obowiązku z art. 33 ust. 1 RODO oraz nie zawiadomił bez zbędnej zwłoki osób, których dane dotyczą, o naruszeniu ochrony ich danych, zgodnie z art. 34 ust. 1 RODO, co oznacza naruszenie przez Bank tych przepisów.

Zgodnie z art. 34 ust. 4 RODO, jeżeli administrator nie zawiadomił jeszcze osób, których dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy - biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko - może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3. Z kolei z treści art. 58 ust. 2 lit. e) RODO wynika, że każdemu organowi nadzorczemu przysługuje uprawnienie naprawcze w postaci nakazania administratorowi zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych.

Ponadto, zgodnie z art. 58 ust. 2 lit. i) RODO, każdemu organowi nadzorczemu przysługuje uprawnienie do zastosowania, oprócz lub zamiast innych środków naprawczych przewidzianych wart. 58 ust. 2 RODO, administracyjnej kary pieniężnej na mocy art. 83 RODO, zależnie od okoliczności konkretnej sprawy.

Prezes UODO stwierdził, że w rozpatrywanej sprawie zaistniały przesłanki uzasadniające nałożenie na Bank administracyjnej kary pieniężnej w oparciu o art. 83 ust. 4 lit. a) RODO.

Prezes UODO podał, że decydując o nałożeniu na Bank administracyjnej kary pieniężnej - stosownie do treści art. 83 ust. 2 lit. a) - k) RODO - wziął pod uwagę następujące okoliczności, stanowiące o konieczności zastosowania w niniejszej sprawie tego rodzaju sankcji oraz wpływające obciążająco na wymiar nałożonej administracyjnej kary pieniężnej:

1. Charakter i waga naruszenia (art. 83 ust. 2 lit. a RODO).

Stwierdzone w niniejszej sprawie naruszenie, polegające na zagubieniu dokumentacji zawierającej dane osobowe klientów Banku w postaci: numeru PESEL wraz z imieniem i nazwiskiem, adresem zameldowania, numerem rachunków bankowych, numerem CIF (numer identyfikacyjny nadawany klientom Banku), ma znaczną wagę i poważny charakter, ponieważ może doprowadzić do szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone, a prawdopodobieństwo ich wystąpienia jest wysokie.

2. Czas trwania naruszenia (art. 83 ust. 2 lit. a RODO).

Za okoliczność obciążającą organ uznał długi czas trwania naruszenia. Od powzięcia przez Bank informacji o naruszeniu ochrony danych osobowych do dnia wydania niniejszej decyzji upłynęły ponad 2 lata, w trakcie których ryzyko naruszenia praw lub wolności osób dotkniętych naruszeniem mogło się zrealizować, a czemu osoby te nie mogły przeciwdziałać ze względu na niewywiązanie się przez Bank z obowiązku zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO oraz z obowiązku powiadomienia osób, których dane dotyczą, w sposób prawidłowy o naruszeniu. Co prawda, administrator zaproponował poszkodowanym skorzystanie, w ramach środków w celu zaradzenia naruszeniu ochrony danych osobowych, z usługi Alert BIK, jednakże w przesłanym piśmie nie wskazał tak istotnych informacji, jak możliwe konsekwencje naruszenia ochrony danych osobowych, czy też imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, od którego osoby te mogłyby uzyskać więcej informacji. W informacji o zagubionych dokumentach brak również wskazania kategorii danych osobowych objętych naruszeniem, które powinien zawierać opis charakteru naruszenia. Administrator w przesłanym piśmie nie podał także środków bezpieczeństwa zastosowanych przez niego w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia.

3. Umyślny charakter naruszenia (art. 83 ust. 2 lit. b RODO).

Zdaniem organu, Bank podjął świadomą decyzję, by nie zawiadamiać o naruszeniu Prezesa UODO, jak i osób, których dane dotyczą. Bank bowiem, przetwarzając dane osobowe na masową skalę, ma wysoki poziom wiedzy w zakresie ochrony danych osobowych, obejmujący wiedzę o konsekwencjach stwierdzenia naruszenia ochrony danych osobowych skutkującego („średnim" w ocenie samego Banku) ryzykiem naruszenia praw i wolności osób fizycznych. Mając taką wiedzę, po dokonaniu analizy ryzyka, Bank wyraził wolę (podjął świadomą i wolną decyzję) rezygnacji z dokonania zgłoszenia naruszenia Prezesowi UODO i powiadomienia osób, których dane dotyczą. Wola ta ujawniona została i konsekwentnie była podtrzymywana przez Bank w postępowaniu prowadzonym przed Prezesem UODO, w trakcie którego organ w pierwszej kolejności informował Bank o obowiązkach ciążących na administratorze w związku z naruszeniem ochrony danych oraz o możliwości wystąpienia w sprawie wysokiego ryzyka naruszenia praw i wolności osób, których dotyczyło naruszenie. W końcu samo

wszczęcie przez Prezesa UODO niniejszego postępowania w przedmiocie obowiązku zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu i zawiadomienia o naruszeniu osób, których dane dotyczą, powinno nasunąć Bankowi, co najmniej wątpliwości co do własnej oceny skutków naruszenia.

4. Stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków (art. 83 ust. 2 lit. f RODO).

Prezes UODO uznał za niezadowalającą współpracę z nim w niniejszej sprawie ze strony Banku. Ocena ta dotyczy reakcji Banku na pisma Prezesa UODO informujące o obowiązkach ciążących na administratorze w związku z naruszeniem ochrony danych, czy wreszcie wobec wszczęcia postępowania administracyjnego w przedmiocie obowiązku zgłoszenia naruszenia ochrony danych osobowych i zawiadomienia o naruszeniu osób, których dane dotyczą.

W ocenie Prezesa Prezes Urzędu Ochrony Danych Osobowych, prawidłowe działania (zgłoszenie naruszenia Prezesowi UODO i zawiadomienie o nim osób, których dotyczyło naruszenie) nie zostały podjęte przez Bank nawet po wszczęciu przez Prezesa UODO postępowania administracyjnego w sprawie.

5. Kategorie danych osobowych, których dotyczyło naruszenie (art. 83 ust. 2 lit. g RODO).

Dane osobowe udostępnione osobie nieuprawnionej nie należą do szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO, jednakże ich szeroki zakres (imię i nazwisko, adres zameldowania, numer PESEL, numery rachunków bankowych oraz numer identyfikacyjny nadawany klientom Banku - numer CIF), wiąże się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.

6. Sposób, w jaki organ nadzorczy dowiedział się o naruszeniu (art. 83 ust. 2 lit. h RODO).

O naruszeniu ochrony danych osobowych stanowiących przedmiot niniejszej sprawy, to jest o zagubieniu przez firmę kurierską DPD dokumentacji, zawierającej dane osobowe przetwarzane przez Bank działający jako administrator tychże danych, Prezes UODO nie został poinformowany zgodnie z przewidzianą dla takich właśnie sytuacji procedurą określoną w art. 33 RODO. Organ za okoliczność obciążającą administratora uznał brak informacji o naruszeniu ochrony danych pochodzących ze strony administratora zobowiązanego do przekazania takiej informacji Prezesowi UODO.

Prezes UODO wskazał, że ustalając wysokość administracyjnej kary pieniężnej, uwzględnił również okoliczności łagodzące, mające wpływ na ostateczny wymiar kary, tj.:

1. Liczba poszkodowanych osób, których dane dotyczą (art. 83 ust. 2 lit. a RODO).

W niniejszej sprawie ustalono, że naruszenie dotyczyło danych osobowych tylko dwóch osób.

Taka liczba osób dotkniętych naruszeniem, szczególnie wobec faktu, że Bank - w związku ze skalą i zakresem swojej działalności - przetwarza dane osobowe bardzo dużej liczby klientów, należy uznać za niewielką, co niewątpliwie stanowi okoliczność łagodzącą w niniejszej sprawie.

2. Działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą (art. 83 ust. 2 lit. c RODO).

Administrator przekazał osobom, których dane dotyczą, pewne informacje dotyczące naruszenia, w tym jego charakter (jednakże bez tak istotnych informacji, jak zakres danych osobowych objętych naruszeniem) i wskazał środki w celu zminimalizowania jego ewentualnych negatywnych skutków, umożliwiając skorzystanie osobom, których dane dotyczą, z bezpłatnej usługi Alert BIK. Takie działanie administratora zasługuje na dostrzeżenie i akceptację, jednakże nie jest w żadnym wypadku równoznaczne ze spełnieniem obowiązku, o którym mowa w art. 34 ust. 1 RODO.

Żadnego wpływu na fakt zastosowania przez Prezesa UODO w niniejszej sprawie sankcji w postaci administracyjnej kary pieniężnej, jak również na jej wysokość, nie miały inne, wskazane w art. 83 ust. 2 RODO, okoliczności.

3. Stopień odpowiedzialności administratora z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez niego na mocy art. 25 i art. 32 (art. 83 ust. 2 lit. d RODO).

Według Prezesa Prezes Urzędu Ochrony Danych Osobowych, naruszenie oceniane w niniejszym postępowaniu (niezgłoszenie Prezesowi UODO naruszenia ochrony danych osobowych oraz niezawiadomienie o naruszeniu ochrony danych osobowych osób, których dane dotyczą) nie ma związku ze stosowanymi przez administratora środkami technicznymi i organizacyjnymi.

4. Wcześniejsze naruszenia przepisów RODO ze strony administratora (art. 83 ust. 2 lit. e RODO).

Organ nie stwierdził wcześniejszych naruszeń przepisów RODO przez Bank w tym zakresie.

5. Przestrzeganie wcześniej zastosowanych w tej samej sprawie środków, o których mowa w art. 58 ust. 2 RODO (art. 83 ust. 2 lit. i RODO).

Prezes UODO nie stosował wcześniej środków, o których mowa we wskazanym przepisie.

6. Stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 RODO lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 RODO (art. 83 ust 2 lit. j RODO).

Administrator nie stosuje zatwierdzonych kodeksów postępowania ani zatwierdzonych mechanizmów certyfikacji.

7. Osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty (art. 83 ust. 2 lit. k).

Organ nie stwierdził, aby administrator osiągnął w związku z naruszeniem jakiekolwiek korzyści lub uniknął strat finansowych.

W ocenie Prezesa Prezes Urzędu Ochrony Danych Osobowych, zastosowana administracyjna kara pieniężna spełnia w ustalonych okolicznościach niniejszej sprawy funkcje, o których mowa w art. 83 ust. 1 RODO, tzn. jest w tym indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca.

Podkreślił, że kara będzie skuteczna, jeżeli jej nałożenie doprowadzi do tego, że Bank, profesjonalnie i na skalę masową przetwarzający dane osobowe, w przyszłości będzie wywiązywał się ze swoich obowiązków z zakresu ochrony danych osobowych, w szczególności w zakresie zgłaszania naruszenia ochrony danych osobowych Prezesowi UODO oraz zawiadamiania o naruszeniu ochrony danych osobowych osób, których dotyczyło naruszenie.

Zdaniem Prezesa UODO, administracyjna kara pieniężna spełni też funkcję represyjną, jako że stanowić będzie odpowiedź na naruszenie przez Bank przepisów RODO. Będzie również spełniać funkcję prewencyjną, wskaże bowiem zarówno Bankowi, jak i innym administratorom danych, na naganność lekceważenia obowiązków administratorów związanych z zaistnieniem naruszenia ochrony danych osobowych, a mających na celu przecież zapobieżenie jego negatywnym i często dotkliwym dla osób, których naruszenie dotyczy, skutkom, a także usunięcie tych skutków lub przynajmniej ograniczenie.

Prezes UODO, mając powyższe na uwadze, na podstawie art. 83 ust. 4 lit. a) w związku z art. 103 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, za naruszenie opisane w sentencji niniejszej decyzji, nałożył na Bank administracyjną karę pieniężną w kwocie 363.832 PLN (słownie: trzysta sześćdziesiąt trzy tysiące osiemset trzydzieści dwa złote, co stanowi równowartość 80.000 EUR).

W ocenie Prezesa UODO, zastosowana kara pieniężna spełnia w ustalonych okolicznościach niniejszej sprawy przesłanki, o których mowa w art. 83 ust. 1 RODO ze względu na powagę stwierdzonego naruszenia w kontekście podstawowego celu RODO - ochrony podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych.

Odnosząc się do wysokości wymierzonej Bankowi administracyjnej kary pieniężnej, uznał, iż jest ona proporcjonalna do sytuacji finansowej Banku i nie będzie stanowiła dla niego nadmiernego obciążenia. Wysokość kary została bowiem określona na takim poziomie, aby z jednej strony stanowiła adekwatną reakcję organu nadzorczego na stopień naruszenia obowiązków administratora, z drugiej jednak strony nie powodowała sytuacji, w której konieczność uiszczenia kary finansowej pociągnie za sobą negatywne następstwa, w postaci znaczącej redukcji zatrudnienia bądź istotnego spadku obrotów Banku.

Zdaniem Prezesa UODO, Bank powinien i jest w stanie ponieść konsekwencje swoich zaniedbań w sferze ochrony danych, o czym świadczy chociażby sprawozdanie finansowe Banku, przesłane do Prezesa UODO w dniu maja 2021 r.

Bank pismem z dnia listopada 2021 r. skierował do Wojewódzkiego Sądu Administracyjnego w Warszawie skargę na decyzję Prezesa UODO z dnia 14 października 2021 r., wnosząc o jej uchylenie w całości i zasądzenie zwrotu kosztów postępowania, w tym kosztów zastępstwa procesowego, według norm przepisanych.

Wnoszący skargę zaskarżonej decyzji zarzucił naruszenie przepisów prawa materialnego, które miało wpływ na wynik sprawy, tj.:

1) art. 33 ust. 1 RODO i art. 34 ust. 1 RODO w zw. z art. 4 pkt 7 RODO polegające na ich błędnej wykładni, a w konsekwencji na niewłaściwym zastosowaniu i błędnym przyjęciu, że Bank był zobowiązany do zgłoszenia naruszenia ochrony danych osobowych do organu i zawiadomienia podmiotów danych o naruszeniu;

2) art. 33 ust. 1 RODO w zw. z art. 4 pkt 12 RODO polegające na ich błędnej wykładni, a w konsekwencji niewłaściwym zastosowaniu i przyjęciu, że Bank miał obowiązek zgłosić do Prezesa UODO zgubienie przesyłki, zawierającej dane osobowe i , przez współpracującą z nim firmę kurierską w sytuacji, gdy zdarzenie to nie stanowiło naruszenia ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO, co doprowadziło do niezasadnego stwierdzenia, że Bank naruszył obowiązek zgłoszenia naruszenia ochrony danych osobowych do organu i zawiadomienia podmiotów danych o naruszeniu i nałożenia na Bank administracyjnej kary pieniężnej;

3) art. 58 ust. 2 lit. e) oraz i) RODO oraz art. 33 ust. 1 RODO, polegające na ich niewłaściwym zastosowaniu i przyjęciu, że Bank miał obowiązek zgłosić do Prezesa UODO zgubienie przesyłki, zawierającej dane osobowe i , przez współpracującą z nim firmę kurierską z uwagi na wysokie ryzyko naruszenia praw i wolności osób fizycznych, w sytuacji, gdy zdarzenie to, nawet w przypadku jego kwalifikacji jako naruszenie ochrony danych osobowych, nie wiązało się z większym niż małe prawdopodobieństwem wystąpienia ryzyka naruszenia praw lub wolności podmiotów danych na poziomie uzasadniającym takie zgłoszenie do organu, co Bank ocenił w wyniku przeprowadzenia prawidłowej analizy ryzyka, wykonanej zgodnie z metodyką Agencji Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA"), rekomendowaną przez Europejską Radę Ochrony Danych (EROD), która wykazała, że powagę naruszenia należy ocenić na poziomie średnim, a w konsekwencji nie jest konieczne zgłoszenie naruszenia do Prezesa UODO, a tym bardziej zawiadomienie podmiotów danych, co doprowadziło do niezasadnego stwierdzenia przez organ, że Bank naruszył obowiązek zgłoszenia naruszenia ochrony danych osobowych do organu i zawiadomienia podmiotów danych o naruszeniu, a następnie do nałożenia na Bank administracyjnej kary pieniężnej;

4) art. 58 ust. 2 lit. e) oraz i) RODO oraz art. 34 ust. 1 RODO, polegające na ich niewłaściwym zastosowaniu i przyjęciu, że Bank miał obowiązek dokonać zawiadomienia wobec i o zgubieniu przesyłki, zawierającej ich dane osobowe, przez współpracującą z nim firmę kurierską, którego nie zrealizował w sytuacji, gdy incydent bezpieczeństwa nie wiązał się z wysokim ryzykiem naruszenia praw i wolności osób fizycznych, a więc takie zawiadomienie nie było konieczne, a pomimo to Bank powiadomił osoby, których dane dotyczą

o incydencie bezpieczeństwa, a także przekazał im informacje, o których mowa w art. 34 ust. 2 RODO, co doprowadziło do niezasadnego stwierdzenia przez organ, że Bank naruszył te przepisy, a następnie do nałożenia na Bank administracyjnej kary pieniężnej;

5) art. 58 ust. 21 lit. e) oraz i RODO oraz art. 33 ust. 1 RODO i art. 34 ust. 1 RODO, polegające na ich niewłaściwym zastosowaniu i przyjęciu, że w przypadku, gdy naruszeniem ochrony danych osobowych objęty jest numer PESEL, zachodzi wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w sytuacji gdy każdorazowe wystąpienie naruszenia ochrony danych osobowych wymaga odrębnej analizy ryzyka w kontekście zmiennych elementów stanu faktycznego, a w konsekwencji objęcie numeru PESEL naruszeniem nie stanowi automatycznie o wysokim poziomie ryzyka, co doprowadziło do niezasadnego stwierdzenia przez organ, że Bank naruszył te przepisy, a następnie do nałożenia na Bank administracyjnej kary pieniężnej;

6) art. 83 ust. 1 w związku z art. 83 ust. 2 lit. a) RODO, polegające na ich niewłaściwym zastosowaniu i przyjęciu, że:

a) naruszenie ma poważny charakter i znaczną wagę, ze względu na fakt, że osoby, których dotyczyło rzekome naruszenie, mogły ponieść szkodę majątkową lub niemajątkową, o której mowa w art. 83 ust. 2 lit. a) RODO, a prawdopodobieństwo ich poniesienia jest wysokie, podczas gdy organ nie stwierdził powstania szkody majątkowej lub niemajątkowej po stronie podmiotów danych, a prawdopodobieństwo jej wystąpienia po upływie ponad 2,5 roku od daty rzekomego naruszenia ochrony danych osobowych jest marginalne,

b) naruszenie ma charakter długotrwały z uwagi na fakt, że w okresie ponad 2 lat od daty rzekomego naruszenia do daty wydania decyzji ryzyko naruszenia praw lub wolności mogło się zrealizować, a osoby, których dane dotyczą nie mogły temu przeciwdziałać z uwagi na niewywiązanie się Banku z właściwego zgłoszenia i zawiadomienia o naruszeniu, podczas gdy naruszenie nie miało długotrwałego charakteru, gdyż Bank niezwłocznie przystąpił do analizy incydentu bezpieczeństwa, a następnie niezwłocznie poinformował podmioty danych o zdarzeniu, pomimo iż w jego ocenie zdarzenie to nie stanowiło naruszenia ochrony danych osobowych, a także nie wiązało się i nadal nie wiąże się z wysokim ryzykiem dla praw i wolności osób, których dane dotyczą, co doprowadziło do nałożenia na Bank administracyjnej kary pieniężnej w nieadekwatnej wysokości, naruszającej zasadę proporcjonalności;

7) art. 83 ust. 1 w zw. z art. 83 ust. 2 lit. b) RODO, polegające na ich niewłaściwym zastosowaniu i uznaniu za okoliczność obciążającą, iż rzekome naruszenie przepisów RODO przez Bank miało charakter umyślny, w sytuacji, w której Bank dokonał prawidłowej analizy incydentu bezpieczeństwa zgodnie z metodyką ENISA rekomendowaną przez EROD, a następnie zgodnie z podejściem opartym na ryzyku podjął pełnoprawną decyzję o niezgłaszaniu naruszenia ochrony danych osobowych do organu, jednocześnie podejmując wszelkie działania, mające na celu zapobieżenie ewentualnym negatywnym skutkom incydentu bezpieczeństwa, w tym kontakt z osobami, których dane dotyczą, co doprowadziło do nałożenia na Bank administracyjnej kary pieniężnej w nieadekwatnej wysokości, naruszającej zasadę proporcjonalności;

8) art. 83 ust. 1 w zw. z art. 83 ust. 2 lit. f) RODO, polegające na ich niewłaściwym zastosowaniu i uznaniu za okoliczność obciążającą co do braku współpracy Banku z organem w celu usunięcia naruszenia lub złagodzenia jego ewentualnych negatywnych skutków, w sytuacji, w której Bank każdorazowo udzielał wyczerpujących wyjaśnień na pytania organu i przedstawiał niezbędne dowody, w terminach wskazanych przez organ, pomimo iż działał w przekonaniu, że incydent bezpieczeństwa nie stanowi naruszenia, a w przypadku jego kwalifikacji jako naruszenia, nie wiąże się on z ryzykiem dla podmiotów danych na poziomie wymagającym zgłoszenia do organu lub podmiotów danych, wobec czego organ nie powinien był traktować tej przesłanki jako okoliczności obciążającej, co doprowadziło do nałożenia na Bank administracyjnej kary pieniężnej w nieadekwatnej wysokości, naruszającej zasadę proporcjonalności;

9) art. 83 ust. 1 w zw. z art. 83 ust. 2 lit. g) RODO, polegające na ich niewłaściwym zastosowaniu i uznaniu za okoliczność obciążającą kategorii danych osobowych objętych rzekomym naruszeniem, w sytuacji gdy naruszenie nie dotyczyło szczególnych kategorii danych ani danych, o których mowa w art. 10 RODO, a zakres danych objętych naruszeniem był wąski i w przypadku jednego z dwóch podmiotów danych, których dotyczyło naruszenie, obejmował jedynie trzy rekordy danych, wobec czego organ nie powinien był traktować tej przesłanki jako okoliczności obciążającej, co doprowadziło do nałożenia na Bank administracyjnej kary pieniężnej w nieadekwatnej wysokości, naruszającej zasadę proporcjonalności;

10) art. 83 ust. 1 w zw. z art. 83 ust. 2 lit d), e) i k) RODO, polegające na ich niewłaściwym zastosowaniu i przyjęciu, że stopień odpowiedzialności Banku

z uwzględnieniem wdrożonych środków technicznych i organizacyjnych, jak również brak wcześniejszego naruszenia ze strony Banku oraz nieosiągnięcie przez Bank bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowych lub uniknięcie przez Bank straty, nie miały żadnego wpływu na wymiar administracyjnej kary pieniężnej nałożonej przez organ na Bank, podczas gdy stanowią one okoliczności łagodzące mające zastosowanie w każdym indywidualnym przypadku naruszenia, w tym odnoszące się do Banku, co doprowadziło do nałożenia na Bank administracyjnej kary pieniężnej w nieadekwatnej wysokości, naruszającej zasadę proporcjonalności;

11) art. 83 ust. 1 RODO, polegające na jego niewłaściwym zastosowaniu i wymierzeniu Bankowi administracyjnej kary pieniężnej za naruszenie przepisów RODO, objętych przepisem art. 83 ust. 4 lit. a) RODO, w celu zniechęcenia innych administratorów do naruszania w przyszłości prawa ochrony danych osobowych, co skutkowało wymierzeniem kary z naruszeniem zasady jej zindywidualizowania i w wysokości nieproporcjonalnej do rzekomego naruszenia przepisów RODO, którego w ocenie organu dopuścił się Bank.

Wnoszący skargę, w uzasadnieniu skargi podniósł, iż Bank nie był zobowiązany do zgłoszenia naruszenia ochrony danych osobowych do organu i zawiadomienia podmiotów danych o naruszeniu. Organ w ogóle nie zajął się ustaleniem jaki - w świetle przepisów RODO - status posiada firma kurierska.

Zdaniem skarżącego, w momencie przejęcia dokumentów, zawierających dane i , administratorem danych zawartych w tych dokumentach stała się DPD. Skoro zatem do ewentualnego naruszenia doszło w trakcie przesyłki (a ustalenia dokonane przez organ temu nie przeczą), to w tym zakresie to DPD powinna wykonać obowiązki, o których mowa w art. 33 ust. 1 i 34 ust. 1 RODO. Argumentując wskazał na wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 15 listopada 2021 r. sygn. II SA/Wa 2465/21.

Wnoszący skargę stwierdził, że nawet gdyby przyjąć, że Bank był administratorem danych w chwili ich zagubienia, to niezasadne jest twierdzenie, że miał obowiązek zgłosić do Prezesa UODO zgubienie przesyłki zawierającej dane osobowe i przez współpracującą z nim firmę kurierską w sytuacji, gdy zdarzenie to nie stanowiło naruszenia ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO w sytuacji, gdy zdarzenie to nawet w przypadku jego kwalifikacji jako naruszenie ochrony danych osobowych, nie

wiązało się z większym niż małe prawdopodobieństwem wystąpienia ryzyka naruszenia praw lub wolności podmiotów danych, co skarżący ocenił w wyniku przeprowadzenia prawidłowej analizy ryzyka.

Bank zakwestionował twierdzenie organu o długotrwałym i umyślnym charakterze naruszenia oraz przyjęcie za okoliczność obciążającą brak współpracy z organem nadzoru.

Zdaniem Banku, administracyjna kara pieniężna została nałożona w nieadekwatnej wysokości z naruszeniem zasady proporcjonalności; wobec nieuwzględnienia istotnych okoliczności łagodzących.

W odpowiedzi na skargę Prezes UODO wniósł o jej oddalenie, podtrzymując stanowisko zajęte w zaskarżonej decyzji. Odnosząc się do zarzutów skargi podniósł m.in., iż to Bank jest administratorem danych i w zakresie, w jakim dokumenty zawierające ich dane uległy zagubieniu w trakcie przesyłki i to Bank zobowiązany był do zgłoszenia naruszenia ochrony danych osobowych. Tylko bowiem nadawca (w przedmiotowej sprawie Bank) posiada wiedzę o tym, jakie dane przekazywane są w przesyłce, a tym samym może ocenić, jakim ryzykiem dla praw lub wolności osoby fizycznej skutkuje utrata przesyłki i ma tym samym możliwość wykonania obowiązku z art. 33 i art. 34 RODO. Operator pocztowy w przedmiotowej sprawie takiej wiedzy nie posiada i posiadać nie może. Zgodnie z art. 41 ust. 1 ustawy Prawo Pocztowe (Dz. U. z 2020 r. poz. 1041 z późn. zm.), operatorzy pocztowi zobowiązani są do ochrony tajemnicy pocztowej obejmującej informacje przekazywane w przesyłkach pocztowych. Mają oni obowiązek zachowania należytej staranności w zakresie uzasadnionym względami technicznymi lub ekonomicznymi przy zabezpieczaniu urządzeń i obiektów wykorzystywanych przy świadczeniu usług pocztowych oraz zbiorów danych przed ujawnieniem tajemnicy pocztowej (art. 41 ust. 6 ustawy Prawo pocztowe). W momencie przyjęcia przesyłki, operator pocztowy ma obowiązek wykonać usługę z należytą starannością i w tym zakresie podlega odpowiedzialności wynikającej z rozdziału 8 ustawy Prawo pocztowe. Podmioty korzystające z usług operatorów pocztowych mają zatem w tym zakresie do dyspozycji określone przepisami prawa środki egzekwowania należytego wykonania umowy o świadczenie usług pocztowych.

Organ, odwołując się do sprawozdania z działalności Prezesa UODO za 2019 r. (https://uodo.gov.pl/437, str. 129-131), wskazał, że w przypadku zagubienia

przesyłki pocztowej obowiązki określone w art. 33 i art. 34 RODO spoczywają na nadawcy przesyłki, ponieważ to on „posiada wiedzę o tym, jakie dane przekazywane są w przesyłce, a tym samym może ocenić, jakim ryzykiem dla praw i wolności osoby fizycznej skutkuje utrata przesyłki" Dla uznania powyższego nie ma żadnego znaczenia, jaki w świetle przepisów RODO, status posiada firma kurierska (czego niezbadanie zarzucił organowi Bank).

Organ zwrócił uwagę, że stanowisko Banku odnośnie tej kwestii jest niezrozumiałe w kontekście zgłaszanych dotychczas przez Bank zgłoszeń naruszeń o analogicznej treści oraz faktu podniesienia braku statusu administratora dopiero na obecnym etapie postępowania, w sytuacji gdy wcześniej nie kwestionował swojego statusu w niniejszej sprawie.

Organ podtrzymał stanowisko, że w przedmiotowej sprawie zaistniały przesłanki, określone w art. 4 pkt 12 RODO, warunkujące uznanie incydentu bezpieczeństwa za naruszenie ochrony danych osobowych. Skoro Bank utracił kontrolę nad przetwarzanymi danymi osobowymi w związku z nieodnalezieniem przesyłki z dokumentami bankowymi zawierającymi dane osobowe jego klientów, to powstało ryzyko nieuprawnionego ujawnienia danych osobowych, czym został naruszony atrybut poufności danych osobowych. Bank nie posiada bowiem wiedzy, co się stało z ww. przesyłką, co jest jednoznaczne z brakiem wiedzy, czy z danymi zawartymi w treści dokumentów, znajdujących się w zaginionej przesyłce, nie zapoznały się osoby nieuprawnione, i co w konsekwencji oznacza, że wystąpiło naruszenie ochrony danych osobowych.

W związku z przedmiotowym naruszeniem ochrony danych osobowych, polegającym na zagubieniu dokumentacji zawierającej dane osobowe klientów Banku, nie jest istotne to, czy nieuprawniony odbiorca faktycznie wszedł w posiadanie i zapoznał się z danymi osobowymi innych osób, lecz to, że wystąpiło takie ryzyko, a w konsekwencji również potencjalnie wystąpiło ryzyko naruszenia praw lub wolności podmiotów danych, które z uwagi na zakres danych należy uznać za wysokie.

Fakt zagubienia przesyłki, zawierającej dokumenty z danymi osobowymi klientów Banku, bezpośrednio naraził ich na możliwość ujawnienia ww. danych osobom nieuprawnionym, a Bank jako administrator nie jest w stanie samodzielnie jednoznacznie stwierdzić, że nie doszło do ujawnienia danych osobowych, dlatego też przedmiotowy incydent traktowany jest jako naruszenie poufności danych

i w zawiadomieniu o naruszeniu skierowanym do osób, których danych osobowych naruszenie dotyczy, powinien znaleźć się opis konsekwencji naruszenia i zalecenia dla tych osób, jak przy ujawnieniu danych osobowych osobie nieuprawnionej.

Organ podkreślił, że Bank w przeprowadzonej ocenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą, przyjął średni poziom tego ryzyka, a określone na tym poziomie ryzyko naruszenia praw lub wolności osób fizycznych nie wyłącza obowiązku, o którym mowa w art. 33 ust. 1 RODO i zobowiązuje do zgłoszenia naruszenia organowi nadzorczemu. Zatem to właśnie Bank wskazał na wystąpienie większego niż małe, tj. średniego, prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności podmiotów danych.

Organ stwierdził, że o nałożeniu administracyjnej kary pieniężnej orzekał przez pryzmat przesłanek wymienionych w art. 83 ust. 1 i ust. 2, a także w art. 33 ust. 1 i art. 34 ust. 1 RODO, wskazując dlaczego zasadnym w przedmiotowej sprawie było zastosowanie właśnie takiego środka naprawczego względem Banku.

Skarżący Bank w replice z dnia marca 2022 r. wywodził, że argumentacja organu zawarta w odpowiedzi na skargę nie zasługuje na uwzględnienie. Nie zgodził się z twierdzeniem, że już samo ryzyko naruszenia poufności, integralności lub dostępności rodzi ryzyko w sferze praw i wolności osób fizycznych. Interpretacja organu w tym względzie wykracza zarówno poza literalne brzmienie, jak i *ratio legis* art. 4 pkt 12 RODO, który to wymaga, aby taki skutek wystąpił.

Bank podniósł, że aby dany incydent bezpieczeństwa został zakwalifikowany jako naruszenie ochrony danych osobowych muszą zostać łącznie spełnione wymienione w RODO warunki, tj. musi dojść do: 1) naruszenia bezpieczeństwa i 2) wystąpienia określonego w art. 4 pkt 12 RODO skutku, np. nieuprawnionego ujawnienia danych. Aby z kolei naruszenie ochrony danych osobowych wymagało notyfikacji do Prezesa UODO (art. 33 RODO), a ewentualnie także do podmiotów danych (art. 34 RODO) - zaistniałe naruszenie musi wiązać się z większym niż małe prawdopodobieństwem, że będzie ono skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (w przypadku notyfikacji do organu) albo z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych (w przypadku notyfikacji do podmiotów danych). Te przesłanki - w odróżnieniu od warunków zawartych w definicji naruszenia ochrony danych osobowych - mają charakter hipotetyczny, tj. w ich przypadku nie ma konieczności, by dane naruszenie praw lub wolności osoby fizycznej ziściło się w rzeczywistości, lecz istotne jest, aby zachodziło określone

prawdopodobieństwo ryzyka lub ryzyko wystąpienia naruszenia w tej sferze. Ocena prawdopodobieństwa lub ryzyka jest zatem wtórna wobec konieczności stwierdzenia, że doszło do naruszenia bezpieczeństwa oraz konkretnego skutku. Kategorie te należy zatem od siebie wyraźnie oddzielić, ponieważ mają one całkowicie odrębny charakter. Zdaniem Banku, naruszenie bezpieczeństwa i jego skutek są to zdarzenia faktyczne, osadzone w rzeczywistości, natomiast ocena prawdopodobieństwa wystąpienia ryzyka, jak i poziomu samego ryzyka naruszenia praw lub wolności osób fizycznych, to działania, które muszą zostać podjęte przez administratora już po stwierdzeniu wystąpienia naruszenia ochrony danych osobowych. Stanowisko organu, zrównujące sytuację, gdy istnieje tylko potencjalne ryzyko utraty poufności danych (jej faktyczne wystąpienie nie jest potwierdzone), z sytuacją, gdy w istocie taki skutek miał miejsce, jest nieuprawnione i stanowi rozszerzającą wykładnię art. 4 pkt 12 w zw. z art. 33 ust. 1 i art. 34 ust. 1 RODO.

Bank zwrócił ponadto uwagę, że proces przesyłania dokumentów za pomocą firmy kurierskiej jest szczególnie skomplikowany z punktu widzenia ochrony danych osobowych. Z jednej strony, jak wskazuje organ, co do zasady wyłącznie nadawca ma wiedzę na temat zawartości przesyłki i przetwarzanych w niej danych. Z drugiej zaś, przekazuje on przesyłkę do doręczenia profesjonalnemu podwykonawcy, na którym spoczywają obowiązki również związane z ochroną zawartości przesyłki oraz danych osobowych, wynikające wprost z przepisów prawa, co często stanowi wyznacznik statusu danego podmiotu jako administratora. Uporczywe pomijanie tej okoliczności przez organ, zarówno w niniejszym postępowaniu, jak i we wszelkich innych jego stanowiskach, przesuwa całkowitą odpowiedzialność za losy przesyłki na nadawcę. W świetle braku jakiejkolwiek kontroli nadawcy nad przesyłką w momencie wydania jej profesjonalnej firmie kurierskiej, zobowiązanej do dochowania określonego poziomu staranności - odpowiedniego dla profesjonalnego podwykonawcy - powyższe stanowisko, zdaniem Banku, nie jest słuszne. W ocenie Banku, organ powinien ponownie przeanalizować powyższy proces i role poszczególnych podmiotów w nim uczestniczących - nie tylko dla potrzeb niniejszej sprawy, ale też *in abstractio,* albowiem problem dotyczy każdego podmiotu nadającego przesyłki, zawierające dane osobowe, w tym samego Prezesa UODO. Kwestia ta nie została dostatecznie wyjaśniona i uargumentowana przez organ, a jej pominięcie w sprawie, w której na Bank została nałożona administracyjna kara

pieniężna w wysokości ponad 350 tys. zł, narusza zasadę pogłębiania zaufania obywateli do państwa (art. 8 k.p.a.).

Powoływanie się przez organ na fakt, że w innych sprawach Bank nie kwestionował statusu operatora pocztowego jest bez znaczenia dla niniejszego postępowania. Sprawy te dotyczyły bowiem innych stanów faktycznych. Co więcej, w przypadku, gdy organ - nawet bez przedstawienia rzetelnego i uargumentowanego stanowiska - przyjmował za pewnik status nadawcy przesyłki, zawierającej dane osobowe, jako administratora, nie odwołując się w ogóle do roli operatora pocztowego, bardziej bezpieczne było dla Banku zgłaszanie naruszeń polegających na zgubieniu przesyłki.

Bank podniósł, że ewentualność wystąpienia szkody jest jednym z czynników, który bada się w ramach oceny wagi naruszenia. Okoliczność, iż w niniejszej sprawie, jak również w innych przytoczonych w skardze postępowaniach, w których Prezes UODO ukarał administratorów administracyjną karą pieniężną, w związku z naruszeniami ochrony danych osobowych, ustalono, że podmioty danych nie poniosły żadnej szkody, pozwala twierdzić, że Prezes UODO błędnie ocenia ten czynnik w ramach analizy wagi naruszenia, nadając mu zbyt duże znaczenie.

Fakt, iż w niniejszej sprawie po ponad 2,5 roku od incydentu bezpieczeństwa nie ponieśli szkody, uwiarygadnia słuszność decyzji Banku w zakresie wykonanej analizy wagi incydentu, jak również oceny braku konieczności zgłoszenia naruszenia do Prezesa UODO. Jednocześnie organ w żaden sposób nie wykazał jakoby obecne ryzyko powstania szkody (czy nawet ryzyko w dacie wydania decyzji) było równe temu z daty zaistnienia incydentu bezpieczeństwa. Takie założenie pozostaje zaś wbrew zasadom logicznego rozumowania i doświadczeniu życiowemu z uwagi na upływ czasu bez oznak jakichkolwiek negatywnych konsekwencji. Jednocześnie, brak szkody jest czynnikiem branym pod uwagę podczas ustalania wysokości administracyjnej kary pieniężnej za naruszenie przepisów RODO. Ważne jest zatem, aby organ prawidłowo interpretował pojęcie szkody. Sam dyskomfort, czy obawy związane z zgubieniem przesyłki, nie stanowią szkody niemajątkowej. W związku z powyższym, brak szkody powinien był zostać w niniejszej sprawie wzięty pod uwagę, jako przesłanka łagodząca wymiar ewentualnej administracyjnej kary pieniężnej.

Zdaniem Banku, nałożona kara pieniężna jest rażąco wysoka również z tego względu, iż uwzględnia element prewencji wobec innych administratorów.

Uwzględnienie tak ukształtowanej przesłanki podczas ustalania wymiaru kary stanowi zaś naruszenie przepisów RODO, które to wskazują, że odstraszający skutek kary (podobnie jak jej inne przesłanki) powinny być odnoszone tylko wobec podmiotu, którego dotyczy sprawa. W konsekwencji organ, odnosząc się do potencjalnego wpływu wysokości kary na innych administratorów, błędnie zastosował tę przesłankę, co doprowadziło do nałożenia kary w wygórowanej wysokości.

Prezes UODO w duplice z dnia czerwca 2022 r. podtrzymał stanowisko wyrażone w zaskarżonej decyzji oraz w odpowiedzi na skargę. Nie zgodził się z twierdzeniem, że zaginięcie przesyłki, zawierającej dokumentację klientów Banku, skutkujące utratą kontroli nad danymi osobowymi, które były w niej zawarte, a jednocześnie wiążące się z konkretnym ryzykiem dla praw lub wolności osób, których dane dotyczą, nie jest zdarzeniem faktycznym, pociągającym za sobą określone skutki.

W takich przypadkach jak ten, którego dotyczy przedmiotowe postępowanie, wbrew twierdzeniom Banku, nie sposób nie opierać się w pewnym zakresie na ryzyku nieuprawnionego wejścia w posiadanie danych osobowych przez osoby trzecie. Przeciwne stanowisko prowadziłoby do sytuacji, w których administratorzy - pomimo utraty kontroli nad danymi osobowymi zawartymi w zagubionych przesyłkach, a tym samym nie mając jakiejkolwiek wiedzy na temat aktualnego miejsca znajdowania się tych danych i tego kto w danym momencie może się z nimi zapoznać – nie traktowaliby tego typu sytuacji jako naruszenia ochrony danych osobowych i nie wywiązywaliby się z ciążących na nich obowiązkach w zakresie zgłoszenia naruszenia ochrony danych osobowych i zawiadomienia o naruszeniu osób, których dane dotyczą. Pozbawiałoby to te osoby ochrony ich praw, uniemożliwiając zarazem podjęcie działań zaradczych i właściwych kroków w tym celu, co w konsekwencji mogłoby prowadzić do szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone.

Zawiadamiając bez zbędnej zwłoki podmiot danych, administrator umożliwia osobie, której dane zostały objęte naruszeniem, podjęcie niezbędnych działań zapobiegawczych w celu ochrony praw lub wolności przed negatywnymi skutkami naruszenia. Art. 34 ust. 1 i 2 RODO ma na celu nie tylko zapewnienie możliwie najskuteczniejszej ochrony podstawowych praw lub wolności podmiotów danych, ale także realizację zasady przejrzystości, która wynika z art. 5 ust. 1 lit. a) RODO.

Właściwe wywiązanie się z obowiązku określonego w art. 34 RODO ma zapewnić osobom, których dane dotyczą, szybką i przejrzystą informację o naruszeniu ochrony ich danych osobowych wraz z opisem możliwych konsekwencji naruszenia ochrony danych osobowych oraz środków, które mogą one podjąć w celu zminimalizowania jego ewentualnych negatywnych skutków. Postępując zgodnie z prawem i wykazując dbałość o interesy osób, których dane dotyczą, Bank powinien był bez zbędnej zwłoki zapewnić osobom, których dane dotyczą, możliwość jak najlepszej ochrony danych osobowych. Dla osiągnięcia tego celu niezbędne jest przynajmniej wskazanie tych informacji, które wymienione są w art. 34 ust. 2 RODO, z którego to obowiązku Bank nie wywiązał się. Bank podejmując zatem decyzję o niezawiadomieniu o naruszeniu organu nadzorczego, jak i osób, których dane dotyczą, w praktyce pozbawił te osoby, przekazanej bez zbędnej zwłoki, rzetelnej informacji o naruszeniu i możliwości przeciwdziałania potencjalnym szkodom.

Wojewódzki Sąd Administracyjny w Warszawie zważył, co następuje:

Skarga nie zasługuje na uwzględnienie, ponieważ Sąd - przeprowadzając kontrolę zgodności z prawem zaskarżonej decyzji Prezesa UODO z dnia 14 października 2021 r., nakładającej na Bank Millenium S.A. z siedzibą w Warszawie, dalej: „Bank", administracyjną karą pieniężną w wysokości 363.832 PLN oraz nakazującej zawiadomienie i o naruszeniu ich danych osobowych w celu przekazania im informacji wymaganych stosownie do art. 34 ust. 2 RODO - nie stwierdził, aby Prezes UODO przy jej wydaniu naruszył przepisy prawa materialnego w stopniu mającym wpływ na wynik sprawy, czy też przepisy postępowania administracyjnego w stopniu mogącym mieć istotny wpływ na wynik sprawy.

Na wstępie podkreślenia wymaga, że kompetencje Prezesa UODO zostały unormowane przede wszystkim w RODO i w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781).

Zadania Prezesa UODO, jako organu właściwego w sprawie ochrony danych osobowych i organu nadzorczego w rozumieniu art. 51 RODO, wymienia art. 57 ust. 1 RODO, przy czym wyliczenie to nie jest wyczerpujące. Katalog środków i uprawnień przysługujących organowi w czasie prowadzonych postępowań oraz uprawnień naprawczych określa art. 58 RODO, a w zakresie nakładania kar pieniężnych - art. 83 RODO.

Stosując przepisy RODO należy mieć na uwadze, że celem tego rozporządzenia (wyrażonym w art. 1 ust. 2) jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych, oraz że ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych (zdanie pierwsze motywu 1 preambuły). W przypadku jakichkolwiek wątpliwości, np. co do wykonania obowiązków przez administratorów - nie tylko w sytuacji, gdy doszło do naruszenia ochrony danych osobowych, ale też przy opracowywaniu technicznych i organizacyjnych środków bezpieczeństwa mających im zapobiegać - należy w pierwszej kolejności brać pod uwagę te wartości.

W zaskarżonej decyzji Prezes UODO zdecydował o nałożeniu oraz wysokości administracyjnej kary pieniężnej w związku z naruszeniem przez Bank podstawowych jego obowiązków, określonych w art. 33 ust. 1 i art. 34 ust. 1 RODO.

Zdaniem Sądu, Prezes UODO dokonał prawidłowej wykładni art. 33 ust. 1 zdanie pierwsze RODO, zgodnie z którym, w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu, zgodnie z art. 55 tegoż rozporządzenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Wbrew twierdzeniom wnoszącego skargę, to Bank jest administratorem danych osobowych, wobec których nastąpiło naruszenie ochrony danych osobowych polegające na zagubieniu dokumentacji, zawierającej dane osobowe klientów Banku.

W zagubionej przesyłce znajdowały się następujące dokumenty: pełnomocnictwo udzielone skarżącemu przez skarżącą, umowa konta oszczędnościowego profit, umowa rachunków bankowych oraz karty debetowej, umowa ramowa o świadczenie usług finansowych, umowa rachunku bankowego, potwierdzenie zmian do umowy rachunku bankowego, umowa karty Millennium Visa Prestige, ankieta inwestycyjna, wynik ankiety inwestycyjnej.

W związku z tym, że są to dokumenty bankowe, nie ma wątpliwości, że administratorem danych widniejących na nich jest Bank, który też nadał przesyłkę, i to Bank zobowiązany był do zrealizowania obowiązków ciążących na administratorze, stosownie do art. 33 ust. 1 i art. 34 ust. 1 RODO. To Bank bowiem,

a nie operator pocztowy, określił cele przetwarzania danych objętych ww. naruszeniem, a także sposoby ich przetwarzania.

W przypadku nieprawidłowości w dostarczaniu przesyłki obowiązek ochrony interesów podmiotu danych z punktu widzenia ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, ciąży na nadawcy przesyłki, który znając zawartość utraconej korespondencji, jest w stanie ocenić zagrożenia wynikające dla osoby, której dane dotyczą. Natomiast operator pocztowy oraz firma kurierska obowiązki administratora, w rozumieniu przepisów RODO, może wykonywać, ale wyłącznie w odniesieniu do danych osobowych nadawców i adresatów przesyłek.

To zatem Bank może ocenić, jakim ryzykiem dla praw lub wolności osoby fizycznej skutkuje utrata przesyłki i w związku z tym ma możliwość wykonania obowiązku w zakresie zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienia o naruszeniu osoby, której dane dotyczą. Firma kurierska takiej wiedzy nie posiada. Tak więc, w przedmiotowej sprawie na Banku spoczywał obowiązek zgłoszenia naruszenia ochrony danych osobowych w trybie art. 33 ust. 1 RODO i zawiadomienia o naruszeniu osób, których dane dotyczą, zgodnie z art. 34 ust. 1 RODO.

W niniejszej sprawie zaistniały przesłanki, określone w art. 4 pkt 12 RODO, warunkujące uznanie incydentu bezpieczeństwa za naruszenie ochrony danych osobowych. Zgodnie bowiem z definicją naruszenia ochrony danych osobowych, zawartą w tym przepisie, naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowanych lub w inny sposób przetwarzanych. Przy czym należy zaznaczyć, że przy interpretacji pojęcia naruszenia ochrony danych osobowych, określonego wyżej powołanym przepisem, nie można pomijać innych przepisów RODO nakładających obowiązki na administratora danych w przypadku wystąpienia takiego naruszenia, tj. art. 33 ust. 1 i art. 34 ust. 1 RODO, które wprost mówią o ryzyku naruszenia praw lub wolności osób fizycznych w związku z naruszeniem ochrony danych osobowych.

W wyniku przedmiotowego zdarzenia, tj. zagubienia przesyłki zawierającej dokumenty z danymi osobowymi klientów Banku, doszło do naruszenia bezpieczeństwa, w wyniku którego powstało ryzyko nieuprawnionego wejścia w posiadanie danych osobowych, a więc ryzyko przypadkowego ich ujawnienia.

Tym samym zostały spełnione przesłanki dla zaistnienia naruszenia ochrony danych osobowych.

Podkreślić należy, że możliwe konsekwencje zaistniałego zdarzenia nie muszą się zmaterializować - w treści art. 33 ust. 1 RODO wskazano, że samo wystąpienie naruszenia ochrony danych osobowych, z którym wiąże się ryzyko naruszenia praw lub wolności osób fizycznych, implikuje obowiązek zgłoszenia naruszenia właściwemu organowi nadzorczemu.

W przedmiotowej sprawie Bank, zgodnie z metodyką opartą na europejskiej metodologii ENISA, ocenił zdarzenie zagubienia przesyłki jako mogące powodować średnie ryzyko naruszenia praw i wolności skarżących, a określone na tym poziomie ryzyko naruszenia praw lub wolności osób fizycznych, nie wyłącza obowiązku, o którym mowa w art. 33 ust. 1 RODO. Bank zatem, stosownie do wyniku własnej analizy ryzyka przeprowadzonej w związku z naruszeniem, powinien dokonać co najmniej zgłoszenia naruszenia organowi nadzorczemu, czego nie uczynił.

Rację ma organ, że brak zgłoszenia naruszenia ochrony danych osobowych pozbawia organ nadzorczy odpowiedniej reakcji na naruszenie, która przejawia się nie tylko w ocenie ryzyka naruszenia dla praw lub wolności osoby fizycznej, ale również w szczególności na weryfikacji, czy administrator zastosował właściwe środki w celu zaradzeniu naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą, jak również, czy zastosował odpowiednie środki bezpieczeństwa w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia.

Zaginięcie przesyłki, zawierającej dokumentację klientów Banku, wbrew twierdzeniom Banku, jest zdarzeniem faktycznym pociągającym za sobą określone skutki. Tym skutkiem jest utrata kontroli nad danymi osobowymi, które się w niej znajdowały, z czym związane jest konkretne ryzyko dla praw lub wolności osób, których dane dotyczą. W związku z zagubieniem danych wystąpiła możliwość ujawnienia ich osobom nieuprawnionym, a to z kolei oznacza naruszenie bezpieczeństwa skutkujące ryzykiem utraty poufności danych osobowych, zaś zakres tych danych wskazuje na wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą.

Należy zgodzić się z Prezesem UODO, że utrata poufności numeru PESEL w połączeniu z danymi osobowymi, takimi jak: imię i nazwisko, adres zameldowania, numery rachunków bankowych oraz numer identyfikacyjny nadawany klientom

Banku - numer CIF, wiąże się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku naruszenia takich danych, jak imię, nazwisko oraz numer PESEL, możliwa jest bowiem kradzież lub sfałszowanie tożsamości skutkująca negatywnymi konsekwencjami dla osób, których dane dotyczą.
Dlatego też Bank w przedmiotowej sprawie powinien był bez zbędnej zwłoki, stosownie do art. 34 ust. 1 RODO, zawiadomić osoby, których dane dotyczą, o naruszeniu ochrony danych osobowych, tak aby umożliwić im podjęcie niezbędnych działań zapobiegawczych. W zawiadomieniu niezbędne jest wskazanie co najmniej tych informacji, które wymienione są w art. 34 ust. 2 RODO, z którego to obowiązku Bank nie wywiązał się. Bank podejmując zatem decyzję o niezawiadomieniu o naruszeniu ochrony danych osobowych organu nadzorczego, jak i osób, których dane dotyczą, w praktyce pozbawił te osoby, przekazanej bez zbędnej zwłoki, rzetelnej informacji o naruszeniu i możliwości przeciwdziałania potencjalnym szkodom.

Przesłana przez Bank do osób, których dane dotyczą, informacja o zagubionych dokumentach nie zawiera elementów, o których mowa w art. 34 ust. 2 RODO, co oznacza w konsekwencji, że nie może zostać uznana za zawiadomienie o naruszeniu ochrony danych osobowych. Prawidłowe zawiadomienie, stosownie do ww. przepisu, powinno bowiem jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO. Natomiast informacja przesłana do klientów Banku zawierała jedynie bardzo ogólny opis charakteru naruszenia (bez wskazania kategorii danych objętych naruszeniem jako istotnego elementu opisu charakteru naruszenia) oraz lakoniczny opis środków w celu zminimalizowania jego ewentualnych negatywnych skutków, który nie pozwalał osobom, których dane objęte zostały naruszeniem, na rzetelną ocenę zaistniałej sytuacji w kontekście zagrożeń dla ich danych osobowych. W ww. piśmie nie umieszczono opisu możliwych konsekwencji, z jakimi wiązać się może przedmiotowe naruszenie ochrony danych osobowych oraz informacji o imieniu i nazwisku oraz danych kontaktowych inspektora ochrony danych lub oznaczeniu innego punktu kontaktowego, od którego można uzyskać więcej informacji. Brak w niej również odniesienia się do środków bezpieczeństwa zastosowanych przez administratora w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia.

Rację ma organ, wskazując, że opis możliwych konsekwencji powinien odzwierciedlać ryzyko naruszenia praw lub wolności tych osób, tak aby umożliwić im podjęcie niezbędnych działań zapobiegawczych. Możliwe konsekwencje powinny mieć charakter opisowy skierowany bezpośrednio do osób. Wskazywane przez administratora możliwe konsekwencje powinny współgrać z proponowanymi środkami minimalizującymi ewentualne negatywne konsekwencje naruszenia dla osób, których dane dotyczą. Ponadto, administrator zobowiązany jest wskazać, jakie działania podjął bądź proponuje podjąć w związku z naruszeniem ochrony danych osobowych. Obowiązkiem administratora jest bowiem zaproponowanie osobom, których dane dotyczą, środków w celu zminimalizowania zaistnienia negatywnych skutków takiego zdarzenia. Zalecenia te powinny mieć formę konkretnych i adekwatnych do danej sytuacji wskazówek, które pozwolą osobom podjąć działania w celu ochrony ich interesów. Zaś ogólnikowa i niepełna informacja w tym zakresie pozbawia osoby, których dane osobowe objęte zostały naruszeniem, podstawowych informacji umożliwiających im realną ocenę zagrożeń i podjęcie racjonalnej decyzji czy i z jakich zaproponowanych przez administratora środków zaradczych skorzystać w celu zminimalizowania negatywnych konsekwencji naruszenia.

Tak więc Prezes UODO prawidłowo ustalił, że Bank nie dokonał zgłoszenia naruszenia ochrony danych osobowych organowi nadzoru w wykonaniu obowiązku z art. 33 ust. 1 RODO oraz nie zawiadomił bez zbędnej zwłoki osób, których dane dotyczą, o naruszeniu ochrony ich danych, zgodnie z art. 34 ust. 1 RODO, co oznacza naruszenie przez Bank tych przepisów.

Jeżeli administrator nie wywiąże się z obowiązku zgłoszenia naruszenia ochrony danych organowi nadzorczemu albo osobom, których dane dotyczą, albo zarówno organowi nadzorczemu, jak i osobom, których dane dotyczą, pomimo spełnienia wymogów ustanowionych w art. 33 lub 34, organ nadzorczy może skorzystać z możliwości, która obejmowałaby wzięcie pod uwagę wszystkich środków naprawczych znajdujących się w jego dyspozycji, co wiąże się z możliwością zastosowania administracyjnej kary pieniężnej w połączeniu ze środkiem naprawczym przewidzianym w art. 58 ust. 2 RODO, albo bez takiego środka. Jeżeli zdecydowano się zastosować administracyjną karę pieniężną, wartość tej kary może opiewać na kwotę do 10 000 000 EUR lub do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego przedsiębiorstwa, zgodnie z art. 83 ust. 4 lit. a) RODO.

Skoro z okoliczności faktycznych sprawy wynika, że Bank naruszył podstawowe obowiązki, przewidziane w art. 33 ust. 1 oraz w art. 34 ust. 1 RODO, to możliwe było zastosowanie art. 83 ust. 2 RODO.

W ocenie Sądu, zastosowana przez Prezesa UODO administracyjna kara pieniężna spełnia, w ustalonych okolicznościach niniejszej sprawy, funkcje, o których mowa w art. 83 ust. 1 RODO, tzn. jest w tym indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca.

Organ wyczerpująco uzasadnił nałożenie administracyjnej kary finansowej, wskazując, określone w art. 83 ust. 1 i ust. 2, a także w art. 33 ust. 1 i art. 34 ust. 1 RODO, przesłanki, na jakich się oparł z uwzględnieniem charakteru, wagi i czasu trwania naruszenia oraz okoliczności zarówno obciążające, jak i łagodzące wymiar tej kary.

W uzasadnieniu zaskarżonej decyzji Prezes PUODO wskazał, na podstawie art. 83 ust. 2 lit. a – k RODO, jakie okoliczności uznał za te, które wpływają na zaostrzenie kary i te, które przemawiają za złagodzeniem wymiaru kary. Nie można więc organowi orzekającemu w sprawie skutecznie postawić zarzutu dowolności podjętego rozstrzygnięcia. Przesłanki, jakie należy wziąć pod uwagę przy nakładaniu przez organ administracyjnej kary pieniężnej, są przesłankami zasadniczo ocennymi. Tak więc, która z przesłanek miarkowania kary jest przesłanką łagodzącą, a która zaostrzającą jej wymiar, jest uzależniona każdorazowo od oceny okoliczności konkretnej sprawy przez organ nadzorczy.

Skoro zatem wszystkie podniesione przez skarżący Bank zarzuty okazały się chybione oraz brak jest podstaw do uznania, że organ dopuścił się innych naruszeń prawa, które mogłyby stanowić o uchyleniu albo stwierdzeniu nieważności zaskarżonej decyzji, Wojewódzki Sąd Administracyjny w Warszawie, na podstawie art. 151 ustawy z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2022 r., poz. 329 z późn. zm.) orzekł jak w wyroku.

Na oryginale właściwe podpisy
Za zgodność z oryginałem

Marcin Rusinowicz-Borkowski

sekretarz sądowy