Warszawa, dnia 14 października 2021 r.

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

DECYZJA

DKN.5131.16.2021

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2021 poz. 735 ze zm.), 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), zwanego dalej również „rozporządzeniem 2016/679”, po przeprowadzeniu postępowania administracyjnego wszczętego z urzędu w sprawie braku zgłoszenia naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych oraz braku zawiadomienia o naruszeniu ochrony danych osobowych osób, których dotyczyło naruszenie, przez Bank Millennium S.A. […], Prezes Urzędu Ochrony Danych Osobowych,

1) stwierdzając naruszenie przez Bank Millennium S.A. […] przepisów:

a) art. 33 ust. 1 rozporządzenia 2016/679, polegające na niezgłoszeniu Prezesowi Urzędu Ochrony Danych Osobowych naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia oraz
b) art. 34 ust. 1 rozporządzenia 2016/679, polegające na niezawiadomieniu o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki osób, których dane dotyczą,

nakłada na Bank Millennium S.A. […] administracyjną karę pieniężną w wysokości 363.832 PLN (słownie: trzysta sześćdziesiąt trzy tysiące osiemset trzydzieści dwa złote),

2) nakazuje Bankowi Millennium S.A. […] zawiadomienie – w terminie 3 dni od dnia doręczenia niniejszej decyzji – Pani M. G. oraz Pana W. G., o naruszeniu ochrony ich danych osobowych w celu przekazania im informacji wymaganych zgodnie z art. 34 ust. 2 rozporządzenia 2016/679, 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.

Uzasadnienie

Do Prezesa Urzędu Ochrony Danych Osobowych, zwanego dalej również ,,Prezesem UODO", dnia […] czerwca 2019 r. wpłynęła skarga Pani M. G. oraz Pana W. G., zwanych dalej: „Skarżącymi", na nieprawidłowości w procesie przetwarzania ich danych osobowych przez Bank Millennium S.A. […], zwany dalej: „Bankiem" lub „Administratorem", polegające na zagubieniu dokumentacji zawierającej dane osobowe Skarżących, przekazanej Bankowi w związku z procedurą założenia konta bankowego w dniu […] marca 2019 r.

Skarżący w treści skargi wskazali, że Oddział Banku w Z. zagubił ich dane osobowe, przekazane w związku z procedurą założenia konta bankowego w dniu […] marca 2019 r. Skarżący wskazali, iż […] maja 2019 r. zostali powiadomieni o zagubieniu dokumentacji zawierającej ich dane osobowe. W dniu […] maja 2019 r. Skarżący udali się do Banku w celu uzyskania dodatkowych informacji w tej sprawie, tj. jak mogą się ustrzec przed ewentualnymi negatywnymi konsekwencjami i co powinni zrobić w zaistniałej sytuacji. Skarżący takich informacji nie uzyskali, w związku z tym dokonali w placówce Banku zgłoszenia reklamacyjnego.

W związku z powyższym, pismem z […] września 2019 r. Prezes UODO, na podstawie art. 58 ust. 1 lit. a) i e) rozporządzenia 2016/679, zwrócił się do Banku o wyjaśnienie, czy w związku z zaistniałym zdarzeniem Bank zgłosił, w trybie art. 33 rozporządzenia 2016/679, Prezesowi UODO naruszenie ochrony danych osobowych w powyższym zakresie, a jeśli tak, to kiedy i czy Bank dopełnił obowiązku zawiadomienia osób, których dane dotyczą, o naruszeniu ich danych osobowych, w myśl art. 34 ust. 1 i 2 rozporządzenia 2016/679. Prezes UODO zwrócił się również o wskazanie, jakich kategorii danych dotyczyło naruszenie, jakie są jego możliwe konsekwencje dla osób, których dane dotyczą oraz czy, a jeśli tak, to jakie Bank zastosował środki zaradcze mające na celu zminimalizowanie ewentualnych negatywnych skutków zaistniałego naruszenia oraz jakie Bank przedsięwziął środki mające na celu niedopuszczenie do zaistnienia w przyszłości naruszeń o podobnym charakterze.

Z odpowiedzi na powyższe, której Bank udzielił pismem z dnia […] października 2019 r. wynika, że 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 […], 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.

Jak wynika ze złożonych wyjaśnień, 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 X Sp. z o.o., zwaną dalej: „X", opóźnienia w doręczeniu ww. przesyłki. Następnie, w dniu […] kwietnia 2019 r. Bank złożył oficjalną reklamację w związku z brakiem doręczenia ww. przesyłki. W dniu […] kwietnia 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.

Mając na uwadze powyższe okoliczności zdarzenia, w tym zakres danych, których dotyczył przedmiotowy incydent, Bank, zgodnie z metodyką opartą na europejskiej metodologii ENISA, ocenił to zdarzenie jako mogące powodować średnie ryzyko naruszenia praw i wolności Skarżących, dlatego też Bank nie zgłosił ww. naruszenia do Prezesa Urzędu Ochrony Danych Osobowych oraz nie zawiadomił osób o naruszeniu ochrony ich danych osobowych zgodnie z art. 34 ust. 1 rozporządzenia 2016/679, wskazując im w przesłanej informacji o zagubionych dokumentach jedynie bardzo ogólne informacje dotyczące charakteru naruszenia (bez wskazania kategorii danych objętych naruszeniem) oraz środki w celu zminimalizowania jego ewentualnych negatywnych skutków, w tym umożliwiając skorzystanie Skarżącym z bezpłatnej usługi Alert […]. Informacja ta nie zawierała natomiast żadnych informacji o konsekwencjach z jakimi wiązać się może przedmiotowe naruszenie ochrony danych osobowych (art. 33 ust. 3 lit. c rozporządzenia 2016/679) oraz informacji, na które wskazuje art. 33 ust. 3 lit. b rozporządzenia 2016/679, tj. imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych lub oznaczenie 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.

Wobec braku zgłoszenia naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych oraz braku zawiadomienia o naruszeniu ochrony danych osobowych osób, których dotyczyło naruszenie, w dniu […] kwietnia 2021 r. Prezes UODO wszczął wobec Banku postępowanie administracyjne w tym przedmiocie.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, pismem z [...] maja 2021 r. Bank przesłał dodatkowe wyjaśnienia, w których wskazał m.in. że:

1. W okresie w którym doszło do zdarzenia objętego skargą obowiązywały jedynie lakoniczne Wytyczne Grupy Roboczej Art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP250rev.01), tj. wytyczne przyjęte w dniu 3 października 2017 r. przez Grupę Roboczą Art. 29 i zatwierdzone następnie przez Europejską Radę Ochrony Danych (zwaną dalej „EROD"), które to wytyczne (zwane dalej „Wytycznymi WP250") zdaniem Banku cyt.: „nie zawierają opinii EROD dla zdarzenia objętego skargą czy nawet zdarzenia w jakikolwiek sposób do niego zbliżonego, a same wskazane w ww. wytycznych przykłady dotyczyły zdarzeń tak poważnych, że mogły sugerować odbiorcom, że notyfikacje na podstawie art. 33 RODO powinny być zarezerwowane właśnie dla szczególnych przypadków";
2. Bank, wskazując na brak w ww. wytycznych, przypadku analogicznego do tego, którego dotyczy niniejsze postępowanie, jednocześnie wskazał, że większość formalnie zagubionych przesyłek pozostaje w stanie nienaruszonym, nie opuszczając infrastruktury dostawców, często bowiem zdarzają się przypadki, kiedy przesyłki spadają z taśmy, co powoduje nadanie im statusu zagubionych;
3. W ocenie Banku, nie w każdym przypadku ujawnienie danych w postaci numeru PESEL powoduje powstanie dużego ryzyka dla praw i wolności osoby poszkodowanej, w tym ryzyka kradzieży tożsamości; trudno też zgodzić się z daleko idącymi konsekwencjami jego ujawnienia jak możliwość zaciągnięcia pożyczki – takie sytuacje w wyniku uzyskania numeru PESEL są rzadkie, o ile w ogóle obecnie możliwe, a ponadto cyt.: „[...] ani banki, ani pożyczkodawcy jako podmioty zobowiązane na podstawie przepisów AML do weryfikacji dokumentu tożsamości nie mogą udzielić finansowania w oparciu o sam numer PSESEL ani numer PESEL w połączeniu z innymi informacjami";
4. Publicznie dostępne są numery PESEL członków organów osób prawnych (np. członków zarządu Banku), jednakże Bank nie ma w związku z tym faktem informacji o wyłudzeniach pożyczek na ich dane, posłużenia się danymi w związku z przyznaniem mandatu, wyłudzenia na ich szkodę środków z ubezpieczenia etc.;
5. Bank zgłasza naruszenia, w wyniku których mogło dojść do ujawnienia danych w tym nr PESEL, jednak nie traktuje tego jako bezwzględnie obowiązującej reguły i nie przyjmuje „globalnych" wytycznych wymuszających zawsze przyjęcie oceny wysokiego ryzyka w przypadku ujawnienia numeru PESEL;
6. Bank powołał się na art. 87 rozporządzenia 2016/679, zgodnie z którym państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym, wskazując jednocześnie, że cyt.: „W przypadku Polski, ustawodawca nie zdecydował się na przyjęcie szczególnych zasad przetwarzania numeru PESEL dla podmiotów prywatnych; pewne szczególne rozwiązania zostały przyjęte w ustawie z dnia 24

września 2010 r. o ewidencji ludności, w rozdziale 6 „Udostępnianie danych z rejestru PESEL oraz rejestrów mieszkańców" dla podmiotów żądających ujawnienia danych z samego rejestru. Nie dotyczy to sytuacji, w których numer PESEL jest ujawniony przez podmiot danych np. w celu zawarcia umowy. Fakt, że ustawodawca nie widzi potrzeby dalszego doszczegółowienia zasad przetwarzania danych z rejestrów sugeruje, że jego przetwarzanie samo w sobie nie powoduje zagrożenia dla obywateli";
7. Bank w wyniku pro konsumenckiej postawy, wyrażającej się dbałością o interesy klientów Banku poinformował Skarżących o zdarzeniu polegającym na zagubieniu przesyłki z dokumentami przez kuriera, załączając do informacji o naruszeniu ochrony danych, pomimo oceny przedmiotowego zdarzenia, jako mającego średni wpływ na prawa i wolności osób, których dane dotyczą, a tym samym niewymagającego notyfikacji do organu nadzorczego, kodu na bezpłatne korzystanie z usługi [...] Alert, jako środka minimalizującego ewentualne negatywne skutki zdarzenia;
8. W ślad za powyższym Bank, po dokonaniu oceny, skutkującej uznaniem średniego ryzyka naruszenia ochrony danych osobowych, pomimo braku takiego obowiązku, z jednej strony chciał zrekompensować poszkodowanym ewentualne niedogodności, z drugiej zapewnić po stronie Banku możliwość reakcji w przypadku gdyby doszło, pomimo niskiego prawdopodobieństwa, do wykorzystania danych Skarżących w systemie bankowym w sposób nieuprawniony;
9. Z informacji Banku wynika, że dane Skarżących nie posłużyły np. do wyłudzenia kredytu, ani próby takiego wyłudzenia, utrata przesyłki nie spowodowała też innych niedogodności, co sugerowałoby poprawność oceny Banku;
10. Bank stale nadzoruje jakość usług oferowanych przez X, monitoruje wykonanie proponowanych działań naprawczych oraz organizuje spotkania w celu omówienia możliwości dalszego doskonalenia procesu, uzyskując informacje na temat szczegółów operacyjnych działań X np. o tym, że wiele z przesyłek uznanych formalnie za zagubione to przesyłki, które np. spadają ze swoich samobieżnych taśm w sortowni, z których odkleiły się etykiety itd., nigdy zatem nie opuszczają infrastruktury X.

Ponadto, do złożonych wyjaśnień Bank załączył dokonaną ocenę pod kątem ryzyka naruszenia praw i wolności osób fizycznych. Na podstawie tej oceny Bank uznał, iż nie doszło do naruszenia skutkującego koniecznością zawiadomienia Prezesa UODO oraz osób, których danych osobowych naruszenie dotyczy. Oceny dokonano posługując się kalkulatorem oceny naruszenia ochrony danych osobowych, który to wypełniony plik wraz z metodyką oceny został przesłany jako dowód wraz z wyjaśnieniami. Ponadto Bank wyjaśnił, iż oblicza ocenę dla incydentu na podstawie takich elementów jak: kontekst przetwarzania danych, łatwość identyfikacji oraz okoliczności naruszenia.

Kontekst przetwarzania danych (DPC) określa rodzaj danych, jakie zostały ujawnione, a także szeregi czynników związanych z ogólnym kontekstem przetwarzania. Łatwość identyfikacji (EI) określa, jak łatwo można wywnioskować tożsamość osób na podstawie danych związanych z incydentem. Okoliczności naruszenia (CB) opisują konkretne okoliczności naruszenia ochrony danych osobowych, głównie związane z naruszeniem bezpieczeństwa i poufności danych, a także wszelkie działania związane z celowym atakiem na infrastrukturę Banku.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Prezes Urzędu Ochrony Danych Osobowych zważył, co następuje:

Zgodnie z art. 4 pkt 12 rozporządzenia 2016/679 „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 rozporządzenia 2016/679 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. 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.

Z kolei art. 34 ust. 1 rozporządzenia 2016/679 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 rozporządzenia 2016/679, 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) rozporządzenia 2016/679, 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.

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) rozporządzenia 2016/679. 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. Podkreślić należy, że **obowiązek zawiadomienia osoby fizycznej o naruszeniu nie jest uzależniony od materializacji negatywnych konsekwencji dla takiej osoby, ale od samej możliwości wystąpienia takiego ryzyka.** Tym samym umożliwia osobie fizycznej dokonanie samodzielnej oceny naruszenia w kontekście możliwości materializacji negatywnych konsekwencji dla takiej osoby i podjęcia decyzji o zastosowaniu lub braku zastosowania działań zaradczych. 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 rozporządzenia 2016/679) oraz osób, których dotyczy naruszenie (art. 34 ust. 1 i 2 rozporządzenia 2016/679), powinna być dokonana przez pryzmat osoby dotkniętej naruszeniem.

Podkreślić należy, 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.** Jak wskazuje Grupa Robocza Art. 29 (tj. Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, powołana na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r., zastąpiona zgodnie z art. 68 rozporządzenia 2016/679 Europejską Radą Ochrony Danych Osobowych, która podczas pierwszego posiedzenia plenarnego EROD zatwierdziła m.in. niżej przywołane wytyczne) w Wytycznych WP250: *„Ryzyko to istnieje w przypadku, gdy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone. Przykłady takich szkód obejmują dyskryminację, kradzież lub sfałszowanie tożsamości, straty finansowe i naruszenie dobrego imienia”*. Nie ulega wątpliwości, że przywołane w wytycznych przykłady szkód, z uwagi na zakres danych objęty niniejszym naruszeniem ochrony danych osobowych, w tym nr PESEL wraz z imieniem i nazwiskiem, adresem, czy numerami rachunków bankowych, mogą wystąpić w omawianym przypadku.

W konsekwencji oznacza to, że występuje wysokie ryzyko naruszenia praw lub wolności osób objętych przedmiotowym naruszeniem, co z kolei skutkuje powstaniem po stronie Banku obowiązku zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, zgodnie z art. 33 ust. 1 rozporządzenia 2016/679, w którym muszą się znaleźć informacje określone w art. 33 ust. 3 rozporządzenia 2016/679 oraz zawiadomienia tych osób o naruszeniu, zgodnie z art. 34 ust. 1 rozporządzenia 2016/679, w którym muszą się znaleźć informacje określone w art. 34 ust. 2 rozporządzenia 2016/679.

Ustosunkowując się do wyjaśnień Banku w pierwszej kolejności wskazać należy, że 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 jako wysokie.** Administrator w swoich wyjaśnieniach podkreślał, że z posiadanych przez niego informacji wynika, że dane nie posłużyły np. do wyłudzenia kredytu ani próby takiego wyłudzenia, utrata przesyłki nie spowodowała też innych niedogodności, dlatego uznał, że naruszenie nie wiąże się z ryzykiem naruszenia praw lub wolności osób nim dotkniętych. Warto podkreślić, że Administrator przewidział jednak, że naruszenie może wiązać się z takim ryzykiem, o czym świadczy fakt

zaproponowania dodatkowej usługi [...] Alert w ramach środków w celu zaradzenia naruszeniu – zdaniem Banku miałoby to umożliwić po jego stronie podjęcie stosownej reakcji w przypadku, gdyby doszło, jak sam wskazuje, *„pomimo niskiego prawdopodobieństwa, do wykorzystania danych Skarżących w systemie bankowym w sposób nieuprawniony”*.

W tym miejscu ponownie wskazać należy, że **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. Podnoszona zatem przez Administratora okoliczność, że cyt.: *„Z informacji Banku wynika, że dane Skarżących nie posłużyły np. do wyłudzenia kredytu ani próby takiego wyłudzenia, utrata przesyłki nie spowodowała też innych niedogodności [...]”* oraz *„do Banku nie została przekazana jakakolwiek informacja o szkodach Skarżących w związku ze zdarzeniem”*, nie ma znaczenia dla stwierdzenia istnienia po stronie administratora obowiązku zgłoszenia przedmiotowego naruszenia ochrony danych osobowych Prezesowi UODO, zgodnie z art. 33 ust. 1 rozporządzenia 2016/679, jak również z uwagi na zakres danych osobowych objętych naruszeniem, zawiadomienia osób, których te dane dotyczą, o naruszeniu.

Jak bowiem stanowi art. 34 ust. 1 rozporządzenia 2016/679, 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 jak wynika z art. 33 ust. 1 rozporządzenia 2016/679, 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. Dokonując oceny pod kątem 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 rozporządzenia 2016/679. Mając na uwadze, że ze względu na zakres ujawnionych danych osobowych wystąpiła możliwość zmaterializowania się doniosłych negatywnych konsekwencji dla osób, których dane dotyczą, to wagę potencjalnego wpływu na prawa lub wolności osób fizycznych należy uznać za wysoką. Jednocześnie prawdopodobieństwo wystąpienia wysokiego ryzyka w następstwie niniejszego naruszenia nie jest małe i nie zostało wyeliminowane. Tym samym ponownie należy wskazać, że w związku z przedmiotowym naruszeniem wystąpiło wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, co w konsekwencji determinuje obowiązek dokonania zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu

oraz zawiadomienia o naruszeniu tych osób. Grupa Robocza Art. 29 w Wytycznych WP250 wskazuje, że *„podczas oceny ryzyka, które może powstać w wyniku naruszenia, administrator powinien łącznie uwzględnić wagę potencjalnego wpływu na prawa i wolności osób fizycznych i prawdopodobieństwo jego wystąpienia. Oczywiście ryzyko wzrasta, gdy konsekwencje naruszenia są poważniejsze, jak również wtedy, gdy wzrasta prawdopodobieństwo ich wystąpienia. W przypadku jakichkolwiek wątpliwości administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna”*. Również w związku z zaistnieniem naruszenia ochrony danych osobowych, nie wystąpiły czynniki obniżające poziom prawdopodobieństwa negatywnych skutków, jak ograniczona możliwość identyfikacji, stwierdzenie, że dane osobowe są publicznie dostępne, czy uznanie niewłaściwego odbiorcy za osobę „zaufaną”.

Brak zgłoszenia przedmiotowego naruszenia ochrony danych osobowych Prezesowi UODO przez Bank jest tym bardziej niezrozumiały, 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, wbrew twierdzeniu Banku, nie wyłącza obowiązku, o którym mowa w art. 33 ust. 1 rozporządzenia 2016/679. Bank zatem stosownie do wyniku własnej analizy ryzyka przeprowadzonej w związku z naruszeniem powinien co najmniej dokonać zgłoszenia naruszenia organowi nadzorczemu, czego, co należy ponownie podkreślić, nie uczynił.

Prezes UODO w publikacji pt. „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych” wskazuje: *„W zależności, z jakim poziomem ryzyka naruszenia praw i wolności osób fizycznych administrator ma do czynienia, inaczej kształtują się jego obowiązki w stosunku do organu nadzorczego, a także osób, których dane dotyczą. Jeżeli w wyniku analizy administrator stwierdził, że prawdopodobieństwo zaistnienia ryzyka naruszenia praw i wolności osób fizycznych jest małe, nie jest on zobligowany do zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych. Wskazane naruszenie musi jedynie wpisać do wewnętrznej ewidencji naruszeń. W przypadku stwierdzenia ryzyka naruszenia praw i wolności osób fizycznych, obowiązkiem administratora jest zgłoszenie naruszenia ochrony danych Prezesowi UODO, jak również umieszczenie wpisu w wewnętrznej ewidencji naruszeń. Wystąpienie wysokiego ryzyka naruszenia praw i wolności osób fizycznych, oprócz wpisu w ewidencji naruszeń, wymaga od administratora podjęcia odpowiednich działań, zarówno wobec organu nadzorczego (zgłoszenie naruszenia ochrony danych), ale także w niektórych przypadkach również wobec osób, których dane dotyczą. W przypadku naruszeń, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, RODO wprowadza bowiem dodatkowy obowiązek niezwłocznego zawiadomienia podmiotu danych*

przez administratora, chyba że ten podjął działania prewencyjne przed zaistnieniem naruszenia albo działania zaradcze po wystąpieniu naruszenia (art. 34 ust. 3 RODO)" (publikacja dostępna na stronie https://uodo.gov.pl/pl/134/1029).

Organ nadzorczy nie podzielił stanowiska Banku zaprezentowanego z piśmie z [...] maja 2021 r., zgodnie z którym Bank stwierdził, że **w praktyce nie jest możliwe wykorzystanie danych z przesyłki zalegającej w magazynie X w stanie nienaruszonym.** Sam fakt nieodnalezienia przesyłki mimo upływu ponad 2 lat od jej zagubienia przez operatora pocztowego oraz to, że de facto X już w dniu [...] maja 2019 r., poinformowała, iż nie zdołała zlokalizować przesyłki i zakończyła próby jej poszukiwania, stanowi wystraczający argument dla uznania, że doszło do naruszenia ochrony danych osobowych i zaistniało ryzyko nieuprawnionego wejścia w posiadanie danych osobowych. Nie do końca zrozumiałe są zatem powody, dla których Bank jest przekonany o tym, że przesyłka znajduje się w sortowni X i „czeka na jej znalezienie".

Dla powyższej oceny nie ma również wpływu fakt, że postępowanie dotyczy ujawnienia danych, które w ocenie Banku w praktyce najprawdopodobniej nigdy nie zostały udostępnione osobom nieuprawnionym i czekają na znalezienie w sortowni X. Ze złożonych wyjaśnień wynika, iż w dniu [...] maja 2019 r. firma kurierska X poinformowała, iż nie zdołała zlokalizować przesyłki i zakończyła próby jej poszukiwania, brak zatem podstaw do tego, aby uznać, że przesyłka z całą pewnością zalega w magazynie X w stanie nienaruszonym i nie jest możliwe wykorzystanie danych w niej zawartych, skoro jej tam nie odnaleziono. Z uwagi na to, że Administrator nie ma wiedzy na temat tego, gdzie aktualnie znajduje się przesyłka i co stało się z zawartymi w niej danymi osobowymi osób, których dane dotyczą, przyjąć należy, że nastąpiło naruszenie bezpieczeństwa skutkujące ryzykiem nieuprawnionego ujawnienia danych osobowych, a zakres tych danych przesądza o tym, że wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Dla lepszego zobrazowania przypadków naruszeń ochrony danych osobowych, gdzie nie występuje obowiązek dokonania zgłoszenia organowi nadzorczemu ze względu na to, iż można uznać, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, można odnieść się do Wytycznych WP250. W wytycznych tych jako przykład naruszenia, które nie wymaga zgłoszenia organowi nadzorczemu wskazano na utratę *„bezpiecznie zaszyfrowanego urządzenia mobilnego, z którego korzystają administrator i jego pracownicy. Zakładając, że klucz kryptograficzny jest bezpiecznie przechowywany przez administratora i nie jest to jedyna kopia danych osobowych, dane osobowe będą niedostępne dla atakującego. Oznacza to, że przedmiotowe naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw i wolności osób, których dane te dotyczą. Jeżeli później okaże się, że klucz kryptograficzny został złamany lub oprogramowanie lub algorytm szyfrujący ma słabe punkty, poziom ryzyka naruszenia praw i wolności osób fizycznych zmieni się wówczas i zgłoszenie może stać się konieczne."* Powyższa sytuacja, w której dane osobowe są

niedostępne dla osoby nieuprawnionej, a ewentualna utrata poufności tych danych uzależniona jest od trudnego do przewidzenia w czasie postępu technologicznego umożliwiającego przełamanie zabezpieczeń kryptograficznych, jest nieporównywalna do sytuacji, w której dokumenty z danymi osobowymi klientów Banku zostały zagubione i pomimo znacznego upływu czasu ich nie odnaleziono. Taka okoliczność inaczej, niż w przypadku bezpiecznego zaszyfrowania danych, nie wyklucza możliwości nieuprawnionego zapoznania się z danymi. Za powyższym przemawia również brak możliwości rzeczywistej weryfikacji, czy dane osobowe nie utraciły atrybutu poufności. Porównując oba przypadki nie można uznać, że przedmiotowe naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych choćby w stopniu zbliżonym do sytuacji wskazanej przez Grupę Roboczą Art. 29 w Wytycznych WP250, co również potwierdza, że nie nastąpiło obniżenie ryzyka do poziomu, w którym można stwierdzić, że jest mało prawdopodobne, by naruszenie skutkowało ryzkiem naruszenia praw lub wolności osoby fizycznej.

Bank w swoich wyjaśnieniach powołał się na przykład nr 15 przedstawiony w Wytycznych Europejskiej Rady Ochrony Danych 01/2021 w sprawie przykładów zgłoszeń naruszeń ochrony danych, wersja 1.0 (dalej również jako „Wytyczne EROD 01/2021”), w którym to przykładzie naruszenie polegało na wysłaniu drogą elektroniczną do 15 nieuprawnionych odbiorców listy 15 gości hotelowych zawierającą ich dane osobowe w zakresie nazwisk, adresów e-mail oraz preferencji żywnościowych (w przypadku dwóch gości). Jak wskazał EROD, w tych konkretnych okolicznościach zagrożenia wynikające z charakteru, wrażliwości, objętości i kontekstu ujawnionych danych są niskie i można stwierdzić, że naruszenie nie miało znaczącego wpływu na osoby, których dane dotyczą. EROD uznał również, że w tym kontekście fakt, że administrator natychmiast skontaktował się z obiorcami po powzięciu wiadomości o błędzie, może zostać uznany za czynnik łagodzący. Bank powołał się na ten przykład gdyż w jego ocenie przedstawiony w nim stan faktyczny jest analogiczny do rozpatrywanego w niniejszej sprawie. Z takim stanowiskiem nie można się jednakże zgodzić gdyż – co zostało wykazane wyżej – w przypadku naruszenia objętego niniejszym postępowaniem ujawniony zakres danych powoduje – w przeciwieństwie do przedstawionego w Wytycznych EROD 01/2021 – wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Za równie nietrafione należy uznać przytoczone w ramach wyjaśnień kolejne przykłady przedstawione w Wytycznych EROD 01/2021, zgodnie z którymi można odstąpić od notyfikacji: przykład nr 9 i przykład nr 13.

W przykładzie nr 13, polegającym na błędnym wysyłaniu przez sprzedawcę detalicznego zarówno zamówień, jak i rachunków, zawierających dane osobowe do niewłaściwych klientów z uwagi na brak szczególnych kategorii danych osobowych lub innych danych, których nadużycie może

prowadzić do istotnych negatywnych skutków, nie wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jednakże w tym przypadku zakres udostępnionych danych zawiera jedynie: imię i nazwisko, adres oraz informacje dotyczące zakupionego przedmiotu i jego ceny.

Zupełnie niezrozumiała jest argumentacja Banku w kontekście braku zasadności zgłoszenia naruszenia ochrony danych osobowych do Prezesa UODO, za którą zdaniem Banku przemawia fakt, że doszło do przesłania danych do błędnego, jednak zaufanego odbiorcy, jakim dla Banku jest X, nawiązując do przykładu nr 9 w Wytycznych EROD 01/2021. W omawianym przykładzie, odnoszącym się do przypadkowego przekazania danych zaufanej stronie trzeciej, nie można doszukać się analogii do niniejszej sprawy, w której **nie mamy do czynienia z przesłaniem danych do zaufanego odbiorcy, bowiem X nie było odbiorcą zagubionej korespondencji, lecz operatorem pocztowym, za pośrednictwem którego Bank wysłał przesyłkę** z dokumentami zawierającymi dane osobowe. Ponadto, również w tym przypadku zakres danych sprowadzający się jedynie do: danych kontaktowych i danych dotyczących samego ubezpieczenia (rodzaj ubezpieczenia, kwota), diametralnie różni się od tego, którego dotyczy przedmiotowe naruszenie ochrony danych.

W tym miejscu przytoczyć należy przykład nr 16 przedstawiony w Wytycznych EROD 01/2021, który jest bliższy przedmiotowemu naruszeniu. Jak wynika z Wytycznych EROD 01/2021 dla tego przykładu, grupa ubezpieczeniowa w ramach oferowania ubezpieczenia samochodowego wysłała do niewłaściwego odbiorcy korespondencję zawierającą dane osobowe w postaci imienia, nazwiska, adresu, daty urodzenia, numeru tablicy rejestracyjnej oraz klasyfikację stawki ubezpieczenia w bieżącym i przyszłym roku. W wytycznych wskazuje się, że niewłaściwy odbiorca powinien zostać poinformowany, że nie może wykorzystywać odczytanych informacji, a mimo tego należy również naruszenie zgłosić organowi nadzorczemu. Także przykład nr 12 odnosi się do naruszenia (kradzież papierowego dziennika z ośrodka odwykowego, w którym to znajdowały się m. in. dane zdrowotne pacjentów przyjętych do placówki), które z uwagi m. in. na zakres ujawnionych kategorii danych osobowych, powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Podkreślić jednak należy, że przykłady z ww. wytycznych nie obejmują kontekstu uwarunkowania krajowego, w którym ujawnienie numeru PESEL wraz z imieniem i nazwiskiem jednoznacznie identyfikuje osobę fizyczną, a w powiązaniu z danymi w zakresie adresu zameldowania, numerów rachunków bankowych, a także numeru CIF (numer identyfikacyjny nadawany klientom Banku) może powodować doniosłe konsekwencje dla osoby, której dane osobowe zostały ujawnione. Odnosząc powyższe do przedmiotowego naruszenia należy wskazać, że obowiązkiem Banku było nie tylko dokonanie zgłoszenia naruszenia ochrony danych Prezesowi UODO, ale również zawiadomienie o naruszeniu osób, których dane dotyczą.

Dla powyższej oceny nie ma także wpływu fakt, że *„Bank obecnie rozważa zmiany w umowie z X, na mocy której X będzie na zlecenie Banku poszukiwać dalej przesyłek Banku uznanych z zaginione”* oraz że z uwagi na stale doskonalony proces obsługi korespondencji w samym Banku *„ostatnio w Banku przygotowano dodatkowe szkolenia z bezpiecznego i poprawnego nadawania przesyłek dla pracowników oddziałów”*. Dane zostały bowiem zagubione, co bezpośrednio naraziło je na możliwość ujawnienia osobom nieuprawnionym, a co z kolei oznacza (co należy ponownie podkreślić), że nastąpiło naruszenie bezpieczeństwa skutkujące ryzykiem utraty poufności danych osobowych, a zakres tych danych, obejmujących również numer ewidencyjny PESEL, przesądza o tym, że wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Analizowanie możliwości zmiany w umowie z X, czy przeprowadzenie przez Administratora dodatkowych szkoleń uznać należy za środek podjęty przez Administratora celem zminimalizowania ryzyka wystąpienia tego typu naruszenia w przyszłości, a nie działanie minimalizujące ryzyko naruszenia praw lub wolności osób fizycznych, których dane dotyczą.

W wyjaśnieniach zawartych w piśmie z […] maja 2021 r. Bank wskazał, iż *„publicznie dostępne są numery PESEL członków organów osób prawnych (np. członków zarządu Banku). Bank nie ma w związku z tym faktem informacji o wyłudzeniach pożyczek na ich dane, posłużenia się danymi w związku z przyznaniem mandatu, wyłudzenia na ich szkodę środków z ubezpieczenia, zawierania umów prawnocywilnych, rejestracji kart pre-paid ani uzyskania wglądu do dokumentacji medycznej. Nie jest możliwe potwierdzenie wykorzystania danych w przypadku budżetów partycypacyjnych, choć podkreślić należy, że wpływ takiego wykorzystania musiałby być minimalny”*. W świetle ww. argumentu Banku wskazać należy, że w przedmiotowej sprawie nie mamy do czynienia z opisaną powyżej sytuacją, dane Skarżących nie są bowiem publicznie dostępne w Monitorze Sądowym i Gospodarczym, czy Krajowym Rejestrze Sądowym. Grupa Robocza Art. 29 w Wytycznych WP250 dla sytuacji, w których zgłaszanie naruszeń nie jest konieczne wskazuje na przykład sytuacji *„w której dane osobowe już są publicznie dostępne i ujawnienie takich danych nie wiąże się z prawdopodobnym ryzykiem dla danej osoby fizycznej.”* Mając na uwadze powyższe, wskazać należy, że w przedmiotowej sprawie taka okoliczność nie wystąpiła, co w konsekwencji nie obniżyło prawdopodobieństwa wystąpienia ryzyka dla osób, których dane dotyczą.

Bank powołuje się także na art. 87 rozporządzenia 2016/679, zgodnie z którym państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym, wskazując jednocześnie, że polski ustawodawca nie zdecydował się na przyjęcie szczególnych zasad przetwarzania numeru PESEL dla podmiotów prywatnych. Zdaniem Banku cyt.: *„pewne szczególne rozwiązania zostały przyjęte w ustawie z dnia 24 września 2010 r. o ewidencji ludności, w rozdziale*

6 „Udostępnianie danych z rejestru PESEL oraz rejestrów mieszkańców" dla podmiotów żądających ujawnienia danych z samego rejestru. Nie dotyczy to sytuacji, w których numer PESEL jest ujawniony przez podmiot danych np. w celu zawarcia umowy. Fakt, że ***ustawodawca nie widzi potrzeby dalszego doszczegółowienia zasad przetwarzania danych z rejestrów sugeruje, że jego przetwarzanie samo w sobie nie powoduje zagrożenia dla obywateli".***

Upublicznianie numeru PESEL, który w Polsce jest krajowym numerem identyfikacyjnym, to dla Prezesa UODO niezwykle ważna kwestia. W tym miejscu Prezes UODO pragnie podkreślić, iż dla przykładu już w 2019 roku, **zwrócił się do Ministra Sprawiedliwości z wystąpieniem o dokonanie zmian w ustawie z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2018 r. poz. 986 z późn. zm.)**. Artykuł 35 pkt 1 tej ustawy zakłada, że ilekroć do Krajowego Rejestru Sądowego wpisuje się osobę fizyczną, zamieszcza się tam nazwisko i imiona oraz identyfikator nadany w systemie ewidencji ludności (numer PESEL). Jednocześnie art. 8 powyższej ustawy zakłada jawność Krajowego Rejestru Sądowego i jego bezwarunkową powszechną dostępność. Prezes UODO w swym wystąpieniu wskazał na konieczność dokonania weryfikacji, funkcjonującej obecnie na gruncie Krajowego Rejestru Sądowego, koncepcji jawności bezwzględnej numeru PESEL. Rozumiejąc przesłanki, dla których numer PESEL funkcjonuje jako dana jawna (bezpieczeństwo obrotu gospodarczego) **wskazał, że rozwiązania te zostały wprowadzone wiele lat temu, a konieczność przestrzegania przepisów rozporządzenia 2016/679 w polskim porządku prawnym sprzyja ponownej weryfikacji tej koncepcji.** Każde podanie numeru PESEL do publicznej wiadomości dotyka również sfery prywatnej osoby. W przypadku Krajowego Rejestru Sądowego dotyczy to również osób, które nie sprawują już funkcji w podmiotach tam uwidocznionych, takich jak byli pełnomocnicy czy byli prokurenci. Numer PESEL osoby ujawniony w Krajowym Rejestrze Sądowym czyni go informacją powszechnie dostępną.

Zgodnie z obecnie obowiązującymi przepisami ujawnianie numeru PESEL w Krajowym Rejestrze Sądowym, a także w kwalifikowanym podpisie elektronicznym, jest dopuszczone ustawowo, niemniej w opinii Prezesa UODO te przepisy, zapewniające legalność takiego przetwarzania danych, powinny być zmodyfikowane, gdyż wzbudzają wątpliwość pod kątem zgodności z art. 87 rozporządzenia 2016/679. Zgodnie z powołanym przepisem państwo może określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego, ale wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie. Biorąc pod uwagę powyższe unormowania Prezes UODO […] czerwca 2019 r. skierował do Ministra Cyfryzacji wystąpienie o dokonanie zmian ustawowych dotyczących kwalifikowanego podpisu elektronicznego. Wskazał, że o ile zasadne jest użycie numeru PESEL w przypadku weryfikacji osoby wnioskującej o wydanie certyfikatu

kwalifikowanego podpisu elektronicznego, o tyle wątpliwości budzi ujawnianie numeru PESEL innym osobom, jako konsekwencja użycia podpisu elektronicznego. Prezes UODO zwrócił uwagę, że przetwarzanie numeru PESEL bez zachowania odpowiednich zasad bezpieczeństwa stwarza szereg zagrożeń dla prywatności osoby fizycznej. Ujawniony w wielu miejscach ułatwia kradzież tożsamości, a także profilowanie osoby bez jej wiedzy i zgody. W odpowiedzi na powyższe wystąpienie organ nadzorczy [...] lipca 2019 r. otrzymał informację, iż Ministerstwo Cyfryzacji deklaruje dokonanie przeglądu regulacji dotyczących identyfikatorów używanych w podpisie elektronicznym.

Biorąc pod uwagę powyższe przykłady działalności Prezesa UODO, który podejmuje możliwe, stosowne kroki mające na celu ochronę krajowego numeru identyfikacyjnego – PESEL, nie ma wątpliwości, że numer PESEL, czyli jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający datę urodzenia, numer porządkowy, oznaczenie płci oraz liczbę kontrolną, a więc ściśle powiązany ze sferą prywatną osoby fizycznej oraz podlegający również, jako krajowy numer identyfikacyjny, wyjątkowej ochronie na gruncie art. 87 rozporządzenia 2016/679, jest daną o szczególnym charakterze i takiej szczególnej ochrony wymaga. Szczególnej ochrony danych osobowych, w tym przede wszystkim numeru ewidencyjnego PESEL wymaga się także od instytucji zaufania publicznego, do których bez wątpienia można zaliczyć stronę przedmiotowego postępowania.

W dalszym ciągu nawiązując do złożonych wyjaśnień, **Administrator brak zgłoszenia zaistniałego naruszenia organowi nadzorczemu argumentuje brakiem istnienia precyzyjnych wytycznych, co do rodzaju naruszeń, które podlegają zgłoszeniu.** Ponadto przykłady naruszeń podlegających zgłoszeniu zamieszczone w Wytycznych WP250 w mniemaniu Administratora dotyczyły zdarzeń tak poważnych, iż odniósł on wrażenie, że obowiązek notyfikacji przewidziany na gruncie art. 33 rozporządzenia 2016/679 zarezerwowany jest dla szczególnych przypadków (Administrator przywołuje przykłady zgłoszonych naruszeń, w których mowa o dużej skali zdarzenia, czy naruszenia dotyczącego szczególnej kategorii danych osobowych – danych medycznych).

W tym miejscu, w pierwszej kolejności należy podkreślić iż, **ani na gruncierozporządzenia 2016/679, ani żadnego innego aktu prawnego, nie funkcjonuje enumeratywne wyliczenie zdarzeń kwalifikowanych jako naruszenie ochrony danych osobowych.** Art. 4 pkt 12 rozporządzenia 2016/679 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. Podkreślić jednocześnie należy, że w Wytycznych WP250, na które powołuje się Administrator, znajdują się rekomendacje Grupy Roboczej Art. 29 dotyczące wymogu zgłaszania naruszeń organowi nadzorczemu.

Z drugiej zaś strony, brak stosownych wytycznych w powyższym zakresie powinien oznaczać, że administrator kierując się koniecznością wywiązania się ze swoich obowiązków, o których mowa w rozporządzeniu 2016/679 oraz dobrem osób, względem których występuje ryzyko naruszenia ich praw lub wolności, będzie zgłaszać organowi nadzorczemu każde zdarzenie, co do którego powstaje wątpliwość, że powodować może jakiekolwiek konsekwencje dla osoby, której dane dotyczą, a także zawiadamiać te osoby o naruszeniach powodujących wysokie ryzyko. Powyższe odnosi się w szczególności do Banku, który będąc podmiotem zaufania publicznego powinien w tym zakresie kreować wyższe standardy.

Przede wszystkim jednak, **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 Urzędu Ochrony Danych Osobowych w roku 2019, były jednymi z najczęstszych, jakie wpływały do organu nadzorczego.

Wskazać bowiem należy, co zresztą jest publikowane na stronie internetowej UODO w rocznych Sprawozdaniach z działalności Prezesa Urzędu Ochrony Danych Osobowych, że **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** *(„Tendencję wzrostową posiadały również zgłoszenia naruszeń ochrony danych osobowych polegające na zagubieniu dokumentacji w formie papierowej przez operatorów pocztowych oraz podmioty świadczące usługi kurierskie. W przypadkach naruszeń ochrony danych osobowych spowodowanych zaginięciem lub nieprawidłowym doręczeniem przesyłek pocztowych, Prezes UODO wskazywał, że to nadawca powinien każdorazowo informować organ nadzorczy o tego rodzaju naruszeniach, jako*

administrator danych osobowych przetwarzanych w związku z realizacją swoich zadań"), **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.

Podkreślić ponownie należy, że oceny ryzyka naruszenia praw lub wolności osoby fizycznej należy dokonać przez pryzmat osoby zagrożonej, a nie interesów administratora. W oparciu o zawiadomienie o naruszeniu osoba fizyczna może sama dokonać oceny, czy w jej opinii incydent bezpieczeństwa może powodować dla niej negatywne konsekwencje i podjąć odpowiednie działania zaradcze. Również w oparciu o informacje przekazane przez administratora dotyczące opisu charakteru naruszenia i zastosowanych lub proponowanych środkach w celu zaradzenia naruszeniu, osoba fizyczna może dokonać oceny, czy po zaistniałym naruszeniu administrator danych nadal daje rękojmię należytego przetwarzania jej danych osobowych w sposób zapewniający ich bezpieczeństwo. W oparciu o taka ocenę może podjąć decyzję np. o rezygnacji z usług administratora lub w przypadku wystąpienia przesłanek, o których mowa w art. 17 rozporządzenia 2016/679, skorzystać z prawa do usunięcia danych. Brak zawiadomienia o naruszeniu osoby fizycznej w przypadku wystąpienia wysokiego ryzyka naruszenia jej praw lub wolności pozbawia ją nie tylko możliwości odpowiedniej reakcji na naruszenie, ale również możliwości dokonania samodzielnej oceny naruszenia, które przecież dotyczy jej danych osobowych i może powodować doniosłe konsekwencje dla niej. Natomiast 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.

Dodatkowo, odnosząc się do konsekwencji, z jakimi może wiązać się ujawnienie nr PESEL, w tym w szczególności kradzieży tożsamości, do której wielokrotnie odwołuje się Administrator w swych wyjaśnieniach, pisząc iż: *„w ocenie Banku nie w każdym przypadku ujawnienie danych w postaci numeru PESEL powoduje powstanie dużego ryzyka dla praw i wolności osoby poszkodowanej, w tym ryzyka kradzieży tożsamości", czy też „ani banki, ani pożyczkodawcy jako podmioty zobowiązane na podstawie przepisów AML do weryfikacji dokumentu tożsamości nie mogą udzielić finansowania w oparciu o sam numer PSESEL ani numer PESEL w połączeniu z innymi informacjami […]",* Prezes UODO pragnie podkreślić, iż **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.

Z całą pewnością w przypadku naruszenia takich danych, jak imię, nazwisko oraz nr PESEL, należy wskazać przede wszystkim na możliwą 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. Co ważne, Bank Millennium S.A. **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 niniejszego postępowania i wskazywanie, że *„takie sytuacje w wyniku uzyskania numeru PESEL są rzadkie, o ile w ogóle obecnie możliwe".***

Podkreślić jeszcze raz należy, że zgłaszając naruszenie organowi nadzorczemu, administratorzy informują Prezesa Ochrony Danych Osobowych, 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) rozporządzenia 2016/679. 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 Urzędu Ochrony Danych Osobowych pozbawiony jest możliwości przeprowadzenia rzetelnej weryfikacji. Grupa Robocza Art. 29 w Wytycznych WP250 wskazuje: *„Zgłaszając naruszenie organowi nadzorczemu, administratorzy mogą zasięgnąć opinii tego organu w kwestii tego, czy w danym przypadku należy przekazać stosowne informacje osobom fizycznym, na które naruszenie wywiera wpływ. Organ nadzorczy może nakazać administratorowi, aby poinformował odpowiednie osoby fizyczne o naruszeniu. Zawiadomienie osób fizycznych o naruszeniu zapewnia administratorowi możliwość przekazania tym osobom informacji na temat ryzyka związanego z naruszeniem oraz wskazania działań, jakie te osoby mogą podjąć, aby uchronić się przed potencjalnymi skutkami naruszenia." „Jednocześnie należy podkreślić, że*

niewywiązywanie się z obowiązku zgłoszenia naruszenia osobie fizycznej albo organowi nadzorczemu może potencjalnie skutkować nałożeniem na administratora kary zgodnie z art. 83".

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.

W motywie 85 preambuły rozporządzenia 2016/679 wyjaśniono: *„Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki.".*

Z kolei w motywie 86 preambuły rozporządzenia 2016/679 wyjaśniono: *„Administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych. Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania. (...)".*

Zawiadamiając bez zbędnej zwłoki podmiot danych, administrator umożliwia osobie podjęcie niezbędnych działań zapobiegawczych w celu ochrony praw lub wolności przed negatywnymi skutkami naruszenia. Art. 34 ust. 1 i 2 rozporządzenia 2016/679 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) rozporządzenia 2016/679

(por. Chomiczewski Witold [w:] RODO. *Ogólne rozporządzenie o ochronie danych. Komentarz.* red. E. Bielak – Jomaa, D. Lubasz, Warszawa 2018). Właściwe wywiązanie się z obowiązku określonego w art. 34 rozporządzenia 2016/679 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 rozporządzenia 2016/679, 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.

W tym miejscu należy podkreślić, że **przesłana do Skarżących przez Bank informacja o zagubionych dokumentach nie zawiera elementów, o których mowa w art. 34 ust. 2 rozporządzenia 2016/679, 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) rozporządzenia 2016/679. 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 umożliwiając skorzystanie Skarżącym z bezpłatnej usługi Alert [...]. 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.

Stosując przepisy rozporządzenia 2016/679 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 konsekwencji należy stwierdzić, że Bank nie dokonał zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu w wykonaniu obowiązku z art. 33 ust. 1 rozporządzenia 2016/679 oraz nie zawiadomił bez zbędnej zwłoki osób, których dane dotyczą, o naruszeniu ochrony ich danych, zgodnie z art. 34 ust. 1 rozporządzenia 2016/679, co oznacza naruszenie przez Bank tych przepisów.

Zgodnie z art. 34 ust. 4 rozporządzenia 2016/679, 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) rozporządzenia 2016/679 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) rozporządzenia 2016/679, każdemu organowi nadzorczemu przysługuje uprawnienie do zastosowania, oprócz lub zamiast innych środków naprawczych przewidzianych w art. 58 ust. 2 rozporządzenia 2016/679, administracyjnej kary pieniężnej na mocy art. 83 rozporządzenia 2016/679, zależnie od okoliczności konkretnej sprawy. Prezes UODO stwierdza, że w rozpatrywanej sprawie zaistniały przesłanki uzasadniające nałożenie na Bank administracyjnej kary pieniężnej w oparciu o art. 83 ust. 4 lit. a) rozporządzenia 2016/679 stanowiący m.in., że naruszenie obowiązków administratora, o których mowa w art. 33 i 34 rozporządzenia 2016/679, podlega administracyjnej karze pieniężnej w wysokości do 10 000 000 EURO, a w przypadku przedsiębiorstwa - w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Stosownie do treści art. 83 ust. 2 rozporządzenia 2016/679, administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a) - h) oraz lit. j) rozporządzenia 2016/679. Decydując o nałożeniu na Bank administracyjnej kary pieniężnej Prezes UODO - stosownie do treści art. 83 ust. 2 lit. a) - k) rozporządzenia 2016/679 - wziął pod uwagę następujące okoliczności sprawy, 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 rozporządzenia 2016/679).
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 rozporządzenia 2016/679).
Za okoliczność obciążającą Prezes UODO uznaje 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 bowiem, Administrator zaproponował poszkodowanym skorzystanie, w ramach środków w celu zaradzenia naruszeniu ochrony danych osobowych, z usługi Alert [...], 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 do środków bezpieczeństwa zastosowanych przez niego w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia.

3. Umyślny charakter naruszenia (art. 83 ust. 2 lit. b rozporządzenia 2016/679).
Zgodnie z Wytycznymi Grupy Roboczej Art. 29 w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia 2016/679 WP253 (przyjętymi w dniu 3 października 2017 r.), zwanymi dalej „Wytycznymi WP253", umyślność „obejmuje zarówno wiedzę, jak i celowe działanie, w związku z cechami charakterystycznymi czynu zabronionego". Bank podjął świadomą decyzję, by nie zawiadamiać o naruszeniu Prezesa UODO, jak i osób, których dane dotyczą. Nie ulega zatem wątpliwości, że Bank, 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 podtrzymywana była przez Bank w postępowaniu prowadzonym przed Prezesem UODO, w trakcie którego Prezes UODO 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. A jak wskazano w Wytycznych WP250, na które sam Bank powołał się w swoich wyjaśnieniach, a co przytoczono już powyżej, „w przypadku jakichkolwiek wątpliwości administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna".

4. Stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków (art. 83 ust. 2 lit. f rozporządzenia 2016/679).

W niniejszej sprawie Prezes UODO uznał za niezadowalającą współpracę z nim 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. Prawidłowe w ocenie Prezesa UODO 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 rozporządzenia 2016/679).

Dane osobowe udostępnione osobie nieuprawnionej nie należą do szczególnych kategorii danych osobowych, o których mowa w art. 9 rozporządzenia 2016/679, 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 rozporządzenia 2016/679).

O naruszeniu ochrony danych osobowych stanowiących przedmiot niniejszej sprawy, to jest o zagubieniu przez firmę kurierską X 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 rozporządzenia 2016/679. Okoliczność braku informacji o naruszeniu ochrony danych pochodzących od administratora zobowiązanego do przekazania takiej informacji Prezesowi UODO należy uznać za obciążającą tego administratora.

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

1. Liczba poszkodowanych osób, których dane dotyczą (art. 83 ust. 2 lit. a rozporządzenia 2016/679).
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 rozporządzenia 2016/679).
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 [...]. 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 rozporządzenia 2016/679.

Żadnego wpływu na fakt zastosowania przez Prezesa Urzędu Ochrony Danych Osobowych w niniejszej sprawie sankcji w postaci administracyjnej kary pieniężnej, jak również na jej wysokość, nie miały inne, wskazane w art. 83 ust. 2 rozporządzenia 2016/679, okoliczności:

1. stopień odpowiedzialności administratora z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez niego na mocy art. 25 i 32 (art. 83 ust. 2 lit. d rozporządzenia 2016/679) - 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;
2. stosowne wcześniejsze naruszenia przepisów rozporządzenia 2016/679 ze strony administratora (art. 83 ust. 2 lit. e rozporządzenia 2016/679) – nie stwierdzono wcześniejszych naruszeń przepisów rozporządzenia 2016/679 przez Bank w tym zakresie;
3. przestrzeganie wcześniej zastosowanych w tej samej sprawie środków, o których mowa w art. 58 ust. 2 rozporządzenia 2016/679 (art. 83 ust. 2 lit. i rozporządzenia 2016/679) - w sprawie Prezes UODO nie stosował wcześniej środków, o których mowa we wskazanym przepisie;
4. stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 rozporządzenia 2016/679 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 rozporządzenia 2016/679 (art. 83 ust 2 lit. j rozporządzenia 2016/679) - administrator nie stosuje zatwierdzonych kodeksów postępowania ani zatwierdzonych mechanizmów certyfikacji;

5. osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty (art. 83 ust. 2 lit. k) - nie stwierdzono, aby administrator osiągnął w związku z naruszeniem jakiekolwiek korzyści lub uniknął strat finansowych.

W ocenie Prezesa UODO zastosowana administracyjna kara pieniężna spełnia w ustalonych okolicznościach niniejszej sprawy funkcje, o których mowa w art. 83 ust. 1 rozporządzenia 2016/679, tzn. jest w tym indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca.

Należy podkreślić, 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.

W ocenie Prezesa Urzędu Ochrony Danych Osobowych administracyjna kara pieniężna spełni funkcję represyjną, jako że stanowić będzie odpowiedź na naruszenie przez Bank przepisów rozporządzenia 2016/679. Będzie również spełniać funkcję prewencyjną; w ocenie Prezesa UODO 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.

Stosownie do treści art. 103 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), równowartość wyrażonych w euro kwot, o których mowa w art. 83 rozporządzenia 2016/679, oblicza się w złotych według średniego kursu euro ogłaszanego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku, a w przypadku gdy w danym roku Narodowy Bank Polski nie ogłasza średniego kursu euro w dniu 28 stycznia - według średniego kursu euro ogłoszonego w najbliższej po tej dacie tabeli kursów Narodowego Banku Polskiego.

Mając powyższe na uwadze, Prezes Urzędu Ochrony Danych Osobowych, 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 – stosując średni kurs euro z dnia 28 stycznia 2021 r. (1 EUR = 4,5479 PLN) – administracyjną karę pieniężną w kwocie 363.832 PLN (co stanowi równowartość 80.000 EUR).

W ocenie Prezesa Urzędu Ochrony Danych Osobowych, zastosowana kara pieniężna w wysokości 363.832 PLN (słownie: trzysta sześćdziesiąt trzy tysiące osiemset trzydzieści dwa złote), spełnia w ustalonych okolicznościach niniejszej sprawy przesłanki, o których mowa w art. 83 ust. 1 rozporządzenia 2016/679 ze względu na powagę stwierdzonego naruszenia w kontekście podstawowego celu rozporządzenia 2016/679 – ochrony podstawowych praw i wolności osób

fizycznych, w szczególności prawa do ochrony danych osobowych. Odnosząc się do wysokości wymierzonej Bankowi administracyjnej kary pieniężnej, Prezes Urzędu Ochrony Danych Osobowych uznał, iż jest ona proporcjonalna do sytuacji finansowej Banku i nie będzie stanowiła dla niego nadmiernego obciążenia. Należy w tym miejscu wskazać, że Bank jest podmiotem dominującym w Grupie Kapitałowej Banku Millennium stanowiącej „przedsiębiorstwo" w rozumieniu motywu 150 rozporządzenia 2016/679. Jak zaś stanowią Wytyczne WP253: „W celu nałożenia skutecznych, proporcjonalnych i odstraszających kar pieniężnych organ nadzorczy stosuje definicję przedsiębiorstwa przyjętą przez TSUE do celów stosowania art. 101 i 102 TFUE, a mianowicie, że poprzez pojęcie przedsiębiorstwa należy rozumieć jednostkę gospodarczą, którą może utworzyć spółka dominująca i wszystkie zaangażowane podmioty zależne." Ze „Skonsolidowanego raportu rocznego Grupy Banku Millennium za rok 2020" zamieszczonego na stronie internetowej Banku [...] wynika, że przychody z działalności podstawowej Grupy Banku Millennium w 2020 r. wyniosły ok. 3,3 mld zł, w związku z czym kwota nałożonej w niniejszej sprawie administracyjnej kary pieniężnej stanowi ok. 0,011 % całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego. Jednocześnie warto podkreślić, że kwota nałożonej kary (363 832,00 zł) to jedynie 0,55 % maksymalnej wysokości kary, którą Prezes UODO mógł – stosując zgodnie z art. 83 ust. 4 rozporządzenia 2016/679 próg 2 % liczony od całkowitego rocznego obrotu – nałożyć na Bank za stwierdzone w niniejszej sprawie naruszenia

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 Urzędu Ochrony Danych Osobowych, 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.

W tym stanie faktycznym i prawnym Prezes Urzędu Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.