PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Warszawa, dnia 30 czerwca 2021 r.

DECYZJA

DKN.5131.11.2020

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2021 r. poz. 735), art. 7 ust. 1 oraz art. 60, art. 101, art. 101a ust. 2 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) i lit. i), art. 83 ust. 1–2 i 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 „rozporządzeniem 2016/679”, po przeprowadzeniu wszczętego z urzędu postępowania administracyjnego 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 Fundację Promocji Mediacji i Edukacji Prawnej Lex Nostra z siedzibą w Warszawie przy ul. Siennej 45 lok. 5, Prezes Urzędu Ochrony Danych Osobowych,

1) stwierdzając naruszenie przez Fundację Promocji Mediacji i Edukacji Prawnej Lex Nostra z siedzibą w Warszawie przy ul. Siennej 45 lok. 5 przepisu 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 przepisu art. 34 ust. 1 rozporządzenia 2016/679, polegające na niezawiadomieniu o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki osób, których dane dotyczą, nakłada na Fundację Promocji Mediacji i Edukacji Prawnej Lex Nostra

z siedzibą w Warszawie przy ul. Siennej 45 lok. 5 administracyjną karę pieniężną w wysokości 13 644 PLN (słownie: trzynaście tysięcy sześćset czterdzieści cztery złote).

2) nakazuje Fundacji Promocji Mediacji i Edukacji Prawnej Lex Nostra z siedzibą w Warszawie przy ul. Siennej 45 lok. 5 zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony danych osobowych zaistniałym w dniu [...] stycznia 2020 r., 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,
w terminie 3 dni od dnia doręczenia niniejszej decyzji,

Uzasadnienie

Fundacja Promocji Mediacji i Edukacji Prawnej LEX NOSTRA z siedzibą w Warszawie, ul. Sienna 45 lok. 5 (zwana dalej „Fundacją"), jest organizacją pożytku publicznego, której statutowe cele obejmują m.in.: udzielanie pomocy prawnej oraz porad prawnych i psychologicznych, pomoc osobom pokrzywdzonym w wyniku przestępstwa oraz ich rodzinom, działania na rzecz ochrony praw osób pokrzywdzonych przez instytucje publiczne, publiczny system ochrony zdrowia oraz podmioty działające w branży ubezpieczeniowej, a także promowanie mediacji w szeroko rozumianym obrocie prawnym i gospodarczym oraz życiu społecznym. Fundacja realizuje swoje cele statutowe udzielając w szczególności osobom fizycznym bezpłatnej pomocy prawnej oraz kierując w ich imieniu i interesie interwencje do odpowiednich organów i instytucji publicznych. W tym zakresie Fundacja przetwarza dane osobowe osób, którym udziela tego rodzaju pomocy.

Do Urzędu Ochrony Danych Osobowych, zwanego dalej również ,,UODO", dnia [...] października 2020 r. wpłynęło „zawiadomienie o podejrzeniu naruszenia zasad przestrzegania przepisów o ochronie danych osobowych" przez Fundację Promocji Mediacji i Edukacji Prawnej LEX NOSTRA z siedzibą w Warszawie, ul. Sienna 45 lok. 5 (zwaną dalej: Fundacją), polegającego na cyt.: „(...) utracie danych osobowych wielu osób, jaka miała miejsce w dniu [...] stycznia 2020 r., na skutek kradzieży teczek zawierających dane osobowe beneficjentów (...)" w mazowieckim biurze terenowym w [...]. Jak wynika z zawiadomienia, kradzież była przedmiotem cyt.: „(...) postępowania karnego prowadzonego przez Prokuraturę Rejonową w [...], sygn.[...], niemniej jednak z analizy przedłożonego postanowienia o umorzeniu dochodzenia wynika, że było ono prowadzone jedynie w kontekście usiłowania popełnienia przestępstwa z art. 279 kk, nie zaś utraty dokumentów zawierających dane osobowe.". W związku z powyższym zaistniała obawa, czy Fundacja w sposób należyty zabezpieczyła dokumenty przed ich utratą oraz administrowała danymi osobowymi w nich zawartymi zgodnie z wymogami rozporządzenia 2016/679.

O podejrzeniu naruszenia zasad przestrzegania przepisów o ochronie danych osobowych organ nadzorczy został poinformowany pismem o sygn. […] z dnia […] października 2020 r. (data prezentaty: […] października 2020 r.) przez Ministerstwo Sprawiedliwości będące organem sprawującym nadzór nad Fundacją.

W związku z powyższym, w dniu […] listopada 2020 r. Prezes Urzędu Ochrony Danych Osobowych, zwany dalej również „Prezesem UODO", na podstawie art. 58 ust. 1 lit. a) i e) rozporządzenia 2016/679, zwrócił się do Fundacji o wskazanie, czy w związku z utratą danych osobowych wielu osób na skutek kradzieży teczek zawierających dane osobowe beneficjentów, naruszenie zostało zgłoszone organowi nadzorczemu, a w przypadku odpowiedzi przeczącej poproszono o przesłanie przeprowadzonej analizy przedmiotowego naruszenia, a także o udzielenie informacji, czy został wyznaczony inspektor ochrony danych, a jeżeli tak, to czy administrator konsultował z inspektorem ochrony danych możliwość zgłoszenia naruszenia organowi nadzorczemu.

W piśmie Prezes UODO wezwał Fundację do złożenia wyjaśnień w terminie 7 dni od dnia otrzymania pisma.

W odpowiedzi na powyższe, Fundacja pismem z dnia […] listopada 2020 r. stwierdziła, iż nie zgłaszała organowi nadzorczemu naruszenia i nie ma wyznaczonego w swojej organizacji inspektora ochrony danych. Ponadto Fundacja wskazała, że dokonana analiza naruszenia dała ocenę jego wagi na poziomie niskim. Na jej podstawie Fundacja uznała, iż nie doszło do naruszenia skutkującego koniecznością zawiadomienia Prezesa UODO.

W związku z ww. pismem, z uwagi na zawartą w nim oceną ryzyka naruszenia praw i wolności osób, których dane dotyczą, Prezes UODO w piśmie z dnia […] listopada 2020 r. wezwał Fundację do wskazania liczby osób, których dotyczyło naruszenie ochrony danych osobowych i kategorii danych osobowych zawartych w utraconej dokumentacji z ich wyszczególnieniem. Wezwał również do wyjaśnienia, czy były przetwarzane szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, oraz dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 rozporządzenia 2016/679, a także w jaki sposób skradziona dokumentacja zawierająca dane osobowe była zabezpieczona przed osobami nieupoważnionymi oraz czy utracona dokumentacja została odtworzona i w jakim terminie, a jeżeli nie, to dlaczego i jaka jest planowana data jej odtworzenia.

W odpowiedzi z dnia […] grudnia 2020 r. Fundacja poinformowała, iż naruszenie dotyczyło 96 osób, utracona dokumentacja zawierała następujące kategorie danych cyt.: „(…) imię, nazwisko, adres do korespondencji, numer telefonu oraz prawdopodobnie numer ewidencyjny PESEL, niemniej wyłącznie 3-4 osoby, których dane osobowe zostały utracone posiadają polskie obywatelstwo, zaś pozostałe osoby nie posiadają polskiego obywatelstwa, a tym samym nie posiadają numeru PESEL", nie były przetwarzane szczególne kategorie danych osobowych, a lokal, w którym była dokumentacja, miał należyte zabezpieczenie w postaci: podwójnego wejścia do lokalu z atestowanymi zamkami, pomieszczenia w lokalu posiadają drzwi zamykane na klucz (oprócz sekretariatu), jest zainstalowany monitoring oraz alarm obsługiwany przez profesjonalną firmę ochroniarską, w lokalu są kasy pancerne oraz szafy zamykane na klucz. W kwestii odtworzenia utraconej dokumentacji Fundacja stwierdziła, iż cyt.: „(…) ze względu na to, że sprawy zostały zamknięte utracona dokumentacja nie podlegała odtworzeniu."

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 [...] grudnia 2020 r. Prezes UODO wszczął wobec Fundacji postępowanie administracyjne (sygnatura pisma:[...]) i wezwał do udzielenia dodatkowych informacji, gdzie konkretnie znajdowały się teczki z danymi osobowymi, czy w przypadku niezabezpieczenia dokumentacji zgodnie z przyjętymi w organizacji zasadami, ustalono osoby odpowiedzialne za naruszenie, czy jest opracowana i wdrożona polityka bezpieczeństwa, a jeżeli tak, to w jaki sposób administrator monitoruje przestrzeganie tych zasad przez pracowników, czy w dniu kradzieży dokumentów zawierających dane osobowe zabezpieczenia były sprawne/działające, użyte zgodnie ze swoim przeznaczeniem (drzwi wejściowe oraz do pozostałych pomieszczeń zamknięte na klucz), uruchomione (monitoring, alarm), jakie przepisy regulują okres przechowywania lub też jego brak, akt osobowych osób, które korzystały z pomocy Fundacji, ewentualnie jakie zostały ustalone przez administratora kryteria okresu przechowywania danych osobowych, jakie obywatelstwo posiadały osoby, niemające numeru ewidencyjnego PESEL, których dane zostały utracone oraz zwrócono się o przesłanie analizy naruszenia uwzględniającej wszelkie kryteria wzięte przez administratora pod uwagę przy ostatecznej ocenie naruszenia praw i wolności osób fizycznych.

Po wszczęciu postępowania administracyjnego w niniejszej sprawie wraz z wezwaniem do udzielenia dodatkowych informacji, pismem z dnia [...] stycznia 2021 r. Fundacja wyjaśniła, iż dokumenty zawierające dane osobowe znajdowały się w lokalu zamykanym na atestowany zamek, objętym monitoringiem, posiadającym włączony alarm, który nadzorowała profesjonalna firma ochroniarska, część teczek była schowana do szafek zamykanych na klucz i w kasie pancernej, a część teczek nie była schowana z uwagi cyt.: „(...) iż były to dokumenty na których pracowano w bieżących sprawach aktualnie prowadzonych przez Fundację (...)", po zaistniałym incydencie administrator przeprowadził rozmowy dyscyplinujące z pracownikami, ma opracowaną i wdrożoną politykę bezpieczeństwa, cyt.: „Administrator wraz z pracodawcą sprawują nadzór nad pracownikami w przedmiocie przestrzegania przez nich powinności pracowniczych, w tym przestrzegania polityki bezpieczeństwa. Po wdrożeniu procedury bezpieczeństwa zorganizowano szkolenie w celu zapoznania pracowników z praktycznymi aspektami stosowania w/w polityki, przewidziano również szkolenia przypominające. W Fundacji stosuje się m.in. zasadę dwóch par oczu — kontrola wew. wychodzącej korespondencji, która służy weryfikacji przekazania na zewnątrz danych osobowych podmiotowi nieuprawnionemu do ich otrzymania, zasada utraty dostępu do danych osobowych dla byłych pracowników, zasada kontroli wyrywkowych — weryfikacja gromadzenia danych przez pracownika, w zakresie zasadności, okresu, ilości danych. Wymaga zaznaczenia, że pracownicy mają świadomość, iż działanie wbrew regulacjom będzie sankcjonowane;", cyt.: „drzwi wejściowe były zamknięte na klucze, kasa pancerna i szafy zamykane na klucz był zamknięte, pozostałe pomieszczenia powinny być zamknięte na klucze, jednakże Fundacja nie jest w stanie tego zweryfikować, monitoring był uruchomiony i poprawnie działał, system alarmowy z uwagi na problemy techniczne związane z pilotem do jego uruchamiania prawdopodobnie nie został uzbrojony jednocześnie wyjaśniamy, iż po kradzieży z włamaniem problemy techniczne z pilotem do uzbrajania systemu alarmowego zostały zweryfikowane z agencją ochrony i wyeliminowane", cyt.: „kryteria przechowywania danych unormowane zostały w Rejestrze Czynności Przetwarzania („RCP"), zawiera on wpis o tym, iż dane będą przechowywane

przez okres wynikający z przepisów prawa, np. w stosunku do archiwizacji dokumentów podatkowych okres przechowywania Danych Osobowych wynosi 5 lat, licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku związany z umową; w stosunku do archiwizacji dokumentów w formie papierowej związanych z udzielaniem pomocy, termin ich przechowywania determinuje czas udzielenia przez Fundację pomocy (kryterium stanowi więc zakończenie udzielania pomocy w jednostkowej sprawie, najczęściej jest to skonstruowanie pism - wezwań do zapłaty, pozwów) lub wycofanie zgody na przetwarzanie. Fundacja wyjaśniła, iż okres przechowywania danych ograniczony jest do minimum, a determinuje go wypełnienie celu, jakim jest zakończenie pomocy prawnej/psychologicznej;", cyt.: „Fundacja nie jest w stanie precyzyjnie określić obywatelstwa osób nieposiadających numeru PESEL, których dane zostały utracone, niemniej będą to osoby z […],[…], […], […] oraz […];". Do pisma z dnia […] stycznia 2021 r. została załączona kopia analizy naruszenia. Fundacja dokonała oceny wagi naruszenia ochrony danych osobowych według Kalkulatora wagi naruszeń ochrony danych osobowych uwzględniającego rekomendacje zawarte w publikacji Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA). Ocena wagi, według Kalkulatora wagi naruszeń ochrony danych osobowych, pozwoliła administratorowi określić poziom dotkliwości naruszenia ochrony danych dla osób, których dane dotyczą, jako niski oraz przyjąć brak obowiązku zgłaszania naruszenia organowi nadzorczemu i zawiadomienia osób o naruszeniu ochrony ich danych.

Do dnia wydania niniejszej decyzji Fundacja nie odzyskała danych osobowych utraconych w wyniku naruszenia stanowiącego przedmiot niniejszego postępowania.

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

W myśl 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 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 (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 rozporządzenia 2016/679 wskazuje, że w sytuacji wysokiego ryzyka dla praw lub 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.

Z treści przywołanych wyżej przepisów rozporządzenia 2016/679 wynika, że w przypadku wystąpienia naruszenia ochrony danych osobowych po stronie administratora danych powstaje obowiązek zgłoszenia go Prezesowi UODO, jeśli z danym naruszeniem wiąże się ryzyko naruszenia praw lub wolności osób fizycznych - niezależnie od poziomu tego ryzyka. Natomiast w sytuacji, gdy naruszenie ochrony danych osobowych powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych administrator danych zobowiązany jest zawiadomić te osoby o naruszeniu ochrony ich danych.

Nie ulega wątpliwości, że zdarzenie polegające na „(...) utracie danych osobowych wielu osób, jaka miała miejsce w dniu [...] stycznia 2020 r., na skutek kradzieży teczek zawierających dane osobowe beneficjentów (...)" z uwagi na zakres danych znajdujących się w utraconej dokumentacji stanowi naruszenie poufności danych ze względu na możliwość zapoznania się z ww. danymi przez osobę (osoby) nieuprawnioną oraz naruszenie dostępności danych w związku z tym, że „(...) utracona dokumentacja nie podlegała odtworzeniu". W konsekwencji należy uznać, że wystąpiło naruszenie bezpieczeństwa prowadzące do przypadkowego utracenia oraz nieuprawnionego dostępu do danych osobowych przetwarzanych przez Fundację, a zatem naruszenie ochrony danych osobowych.

Z ryzykiem naruszenia praw lub wolności osób fizycznych mamy do czynienia wówczas, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Podkreślić należy, że możliwe konsekwencje zaistniałego zdarzenia nie muszą się zmaterializować - w treści art. 33 ust. 1 rozporządzenia 2016/679 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. Podobnie jest w przypadku art. 34 ust. 1 rozporządzenia 2016/679 – dla powstania obowiązku zawiadomienia osoby, której dane dotyczą, o naruszeniu wystarcza, że naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności tych osób.

Wartościami, na jakie rozporządzenie 2016/679 kładzie szczególny nacisk w zakresie szacowania ryzyka, są zatem prawa lub wolności osób, których dane dotyczą i te wartości należy mieć przede wszystkim na uwadze, oceniając ryzyko związane z przetwarzaniem danych osobowych. Zgodnie z motywem 2 preambuły rozporządzenia 2016/679, zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób – naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych. Prawo to jest bowiem prawem podstawowym gwarantowanym art. 8 Karty Praw Podstawowych i musi być respektowane w przypadku prowadzania każdej bez wyjątku operacji przetwarzania danych. Mówiąc o ryzyku naruszenia praw lub wolności osób fizycznych na gruncie rozporządzenia 2016/679, konieczne jest uwzględnienie: 1) prawdopodobieństwa wystąpienia określonego zdarzenia będącego naruszeniem, oraz 2) powagi tego zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą. Natomiast motyw 76 rozporządzenia 2016/679 wskazuje, że prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić przez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej i rzeczowej analizy, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko. Nie bez znaczenia dla oceny sytuacji pozostaje fakt, iż Fundacja nie jest w stanie dokładnie wskazać kategorii danych osobowych zawartych w utraconej dokumentacji, co mogło przyczynić się do niewłaściwego oszacowania przez nią ryzyka naruszenia, cyt.: „(...) kategorie danych osobowych w utraconej dokumentacji to m.in. imię, nazwisko, adres do korespondencji, numer telefonu oraz prawdopodobnie numer PESEL, niemniej wyłącznie 3-4 osoby, których dane osobowe zostały utracone posiadają polskie obywatelstwo, zaś pozostałe osoby nie posiadają polskiego obywatelstwa, a tym samym nie posiadają numeru PESEL;”. Jednocześnie, ze zgromadzonego materiału dowodowego nie wynika, aby Fundacja podejmowała jakiekolwiek działania w celu zweryfikowania faktycznego zakresu danych osobowych znajdujących się w skradzionej dokumentacji oraz czy rzeczywiście nr PESEL dotyczył tylko 3 – 4 osób. Brak takiej weryfikacji powoduje zwiększenie poziomu ryzyka naruszenia praw lub wolności tych osób. W wyniku jej przeprowadzenia mogłoby się bowiem okazać, że zakres danych osobowych, do których uzyskała dostęp osoba (lub osoby) nieuprawniona jest szerszy niż wskazywany przez Fundację, choćby z uwagi na to, że w związku z udzielaniem pomocy prawnej / psychologicznej Fundacja mogła pozyskać dane niezbędne do prawidłowego udzielenia takiej pomocy, inne niż wymienione w złożonych przez nią wyjaśnieniach.

W tym kontekście podnieść należy, że przedstawiona przez Fundację analiza ryzyka stanowiąca załącznik do jej wyjaśnień, to w rzeczywistości wydruk z kalkulatora wagi naruszeń ochrony danych osobowych udostępnianego na stronie internetowej jednego z podmiotów świadczących usługi wsparcia w zakresie ochrony danych osobowych. Prezes UODO nie ocenia w tym miejscu poprawności działania wskazanego kalkulatora, zaznaczając jednak, że za pomocą kalkulatorów możliwe jest uzyskanie dowolnego wyniku, w zależności od danych wprowadzonych do obliczeń. Ponadto na przedmiotowych wydrukach zawarte jest zastrzeżenie, „że każdy przypadek naruszenia, bądź podejrzenia naruszenia ochrony danych osobowych powinien być analizowany indywidualnie, w szczególności w zakresie obowiązków określonych w art. 33 i 34 RODO, z tego względu niniejszy kalkulator może stanowić co najwyżej dodatkowe źródło pomocnicze i nie może być samodzielną

podstawą podejmowania decyzji przez jakikolwiek podmiot lub osobę, które korzystają z kalkulatora na własną odpowiedzialność". Ponadto dokumenty te nie są opatrzone w datę wytworzenia, ani nie zawierają opisu szczegółowych kryteriów, jakimi kierowała się Fundacja dokonując oceny za pomocą wskazanego kalkulatora. Przedstawiony przez Fundację wydruk, zgodnie zresztą z zastrzeżeniem dostawcy na nim zawartym, może mieć zatem jedynie pomocniczy charakter i nie może stanowić podstawy dokonania oceny ryzyka naruszenia praw lub wolności osób fizycznych.

Podkreślić należy, że naruszenie poufności danych, jakie wystąpiło w przedmiotowej sprawie, w związku z naruszeniem ochrony danych osobowych polegającym na cyt.: „(...) utracie danych osobowych wielu osób, jaka miała miejsce w dniu [...] stycznia 2020 r., na skutek kradzieży teczek zawierających dane osobowe beneficjentów (...)", w szczególności danych dotyczących numerów ewidencyjnych PESEL wraz z imionami i nazwiskami, adresami korespondencyjnymi, numerami telefonów, powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Jak wskazuje Grupa Robocza Art. 29 w wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, zwanych dalej również ,,wytycznymi": „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 mogą wystąpić w omawianym przypadku. Nie bez znaczenia dla takiej oceny jest możliwość łatwej w oparciu o ujawnione dane identyfikacji osób, których dane zostały objęte naruszeniem. W konsekwencji oznacza to, że występuje wysokie ryzyko naruszenia praw i wolności osób objętych przedmiotowym naruszeniem, co z kolei skutkuje powstaniem po stronie Fundacji 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.

W sytuacji, gdy na skutek naruszenia ochrony danych osobowych, występuje wysokie ryzyko naruszenia praw i 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. (...)".*

Fundacja podejmując zatem decyzję o niezawiadomieniu o naruszeniu organu nadzorczego, jak i osób, których dane dotyczą, w praktyce pozbawiła te osoby możliwości przeciwdziałania potencjalnym szkodom. 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, administrator 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 administrator nie wywiązał się.

Co do zasady administrator powinien zawiadomić indywidualnie osoby, których dane dotyczą, o naruszeniu ochrony danych osobowych. Jeżeli jednak Fundacja nie posiada kopii skradzionych dokumentów, nie jest w stanie ich odtworzyć lub nie przetwarza tych danych przy użyciu systemu informatycznego, i tym samym nie jest w stanie zidentyfikować osób, których dane dotyczą, to stosownie do art. 34 ust. 3 lit. c) rozporządzenia 2016/679 powinna dokonać zawiadomienia tych osób poprzez wydanie publicznego komunikatu lub zastosowanie podobnego środka, aby w równie skuteczny sposób poinformować osoby, których dane dotyczą, o naruszeniu.

Administrator 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.

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 Administrator 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 Administratora tych przepisów.

Zgodnie z art. 34 ust. 4 rozporządzenia 2016/679, jeżeli administrator nie zawiadomił jeszcze osoby, której 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 osoby, której dane dotyczą, o naruszeniu ochrony danych.

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 Fundację 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 EUR, 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 Fundację 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 kary pieniężnej:

a) Charakter i waga naruszenia (art. 83 ust. 2 lit. a rozporządzenia 2016/679).
Stwierdzone w niniejszej sprawie naruszenie 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. Wysokie ryzyko wystąpienia negatywnych konsekwencji dla osób, których dane zostały przez Fundację utracone, a tym samym wagę naruszenia, potwierdzają okoliczności zdarzenia mającego miejsce [...] stycznia 2020 r., w szczególności to, że nie było to przypadkowe zdarzenie, a celowe działanie osoby lub osób trzecich (nieznanych ani Fundacji, ani Prezesowi UODO, ani organom ścigania prowadzącym postępowanie w sprawie kradzieży) działających w sposób przestępny i co do których założyć należy – w związku z takim sposobem działania – złą wolę jako motyw tego działania.

b) Czas trwania naruszenia (art. 83 ust. 2 lit. a rozporządzenia 2016/679).
Czas trwania naruszenia przepisu art. 34 ust. 1 rozporządzenia 2016/679 jest w ocenie Prezesa UODO bardzo długi. Od powzięcia przez Fundację informacji o naruszeniu ochrony danych osobowych ([...] stycznia 2020 r.) do chwili obecnej (naruszenie nie zostało usunięte) upłynęło piętnaście miesięcy, w trakcie których ryzyko naruszenia praw lub wolności osób dotkniętych naruszeniem mogło się zrealizować, a czemu osoby te nie mogłyby przeciwdziałać ze względu na niewywiązanie się przez Fundację z obowiązku powiadomienia ich o naruszeniu. Za długi Prezes UODO uznaje również czas trwania naruszenia przepisu art. 33 ust. 1 rozporządzenia 2016/679, jakkolwiek ostatecznie Fundacja – w odpowiedzi na trzy kierowane do niej wezwania i po upływie dwunastu miesięcy od powzięcia informacji o naruszeniu ochrony danych osobowych - udzieliła Prezesowi UODO informacji wyczerpujących treść zgłoszenia, o której mowa w art. 33 ust. 3 rozporządzenia 2016/679, w związku z czym Prezes UODO stwierdza, że stan naruszenia art. 33 ust. 1 został usunięty.

c) Liczba poszkodowanych osób, których dane dotyczą (art. 83 ust. 2 lit. a rozporządzenia 2016/679).
W niniejszej sprawie ustalono, że naruszenie dotyczyło danych osobowych wielu osób – na skutek kradzieży teczek zawierających dane osobowe beneficjentów – to jest 96 osób, które korzystały z pomocy prawnej w Fundacji.

d) Umyślny charakter naruszenia (art. 83 ust. 2 lit. b rozporządzenia 2016/679).
Fundacja podjęła świadomą decyzję, by nie zawiadamiać o naruszeniu Prezesa UODO, jak i osób, których dane dotyczą, pomimo powzięcia informacji o utracie danych osobowych wielu osób na skutek kradzieży teczek zawierających dane osobowe, lekceważąc również kierowane do niej pisma Prezesa UODO wskazujące na ciążące na administratorze obowiązki wynikające z przytoczonych wyżej art. 33 ust. 1 i 3 oraz art. 34 ust. 1 i 2 rozporządzenia 2016/679.

e) 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 Fundacji. Ocena ta dotyczy reakcji Fundacji na pisma Prezesa UODO wskazujące na obowiązki administratora wynikające z art. 33 i art. 34 rozporządzenia 2016/679. Jak wskazano wyżej (w odniesieniu się do przesłanki z art. 83 ust. 2 lit. a – „Czas trwania naruszenia") stan naruszenia

przepisu art. 34 ust. 1 został usunięty, aczkolwiek uzyskanie od Fundacji informacji odpowiadających minimalnemu zakresowi zgłoszenia określonemu w art. 33 ust. 3 rozporządzenia 2016/679 wymagało kilkukrotnego skierowania do niej pism informujących o ciążących na administratorze obowiązkach oraz wzywających do udzielenia wyjaśnień, a na dalszym etapie postępowania – do uzupełnienia i sprecyzowania już przekazanych Prezesowi UODO informacji. Natomiast w zakresie wypełnienia obowiązku zawiadomienia o naruszeniu osób, których dane dotyczą (a więc usunięcia stanu naruszenia przepisu art. 34 ust. 1 rozporządzenia 2016/679) do chwili obecnej nie zostały przez Fundację podjęte żadne działania, pomimo formalnego wszczęcia przez Prezesa UODO postępowania administracyjnego w sprawie.

Ustalając wysokość administracyjnej kary pieniężnej, Prezes UODO nie miał podstaw do uwzględnia okoliczności łagodzących, które mogłyby mieć wpływ na ostateczny wymiar kary.

Żadnego wpływu na fakt zastosowania przez Prezesa Urzędu 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:
a) 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;
b) stosowne wcześniejsze naruszenia przepisów rozporządzenia 2016/679 dokonane przez Fundację (art. 83 ust. 2 lit. e rozporządzenia 2016/679) – nie stwierdzono ze strony Fundacji żadnych stosownych wcześniejszych naruszeń rozporządzenia 2016/679;
c) 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 niniejszej sprawie nie zastosowano wcześniej wobec Fundacji środków, o których mowa w art. 58 ust. 2 rozporządzenia 2016/679;
d) 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) - Fundacja nie stosuje zatwierdzonych kodeksów postępowania ani zatwierdzonych mechanizmów certyfikacji, o których mowa w przepisach rozporządzenia 2016/679;
e) osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty (art. 83 ust. 2 lit. k) – na dzień wydania niniejszej decyzji Prezes UODO nie stwierdził, żeby dopuszczając się naruszenia podlegającego karze Fundacja osiągnęła jakiekolwiek korzyści finansowe lub uniknęła jakichkolwiek strat finansowych;
f) kategorie danych osobowych, których dotyczyło naruszenie (art. 83 ust. 2 lit. g rozporządzenia 2016/679) - dane osobowe utracone na skutek kradzieży teczek nie należą do szczególnych kategorii danych osobowych, o których mowa w art. 9 rozporządzenia 2016/679, jednakże połączenie kilku rodzajów danych osobowych (imię, nazwisko, adres do korespondencji, numer telefonu oraz prawdopodobnie numer ewidencyjny PESEL), wiąże się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.

g) 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 cyt.: „(...) utracie danych osobowych wielu osób, jaka miała miejsce w dniu [...] stycznia 2020 r., na skutek kradzieży teczek zawierających dane osobowe beneficjentów (...)", przetwarzanych przez Fundację działającą jako administrator tychże danych, Prezes UODO nie został poinformowany zgodnie z przewidzianą dla takich właśnie sytuacji procedurą określoną w art. 33 rozporządzenia 2016/679. Zawiadomienie w tej sprawie złożył Prezesowi UODO Minister Sprawiedliwości sprawujący w ramach swoich kompetencji nadzór nad działalnością Fundacji.

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 Fundacja, profesjonalnie i na skalę masową przetwarzająca dane osobowe, w przyszłości będzie wywiązywała 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. Zastosowanie administracyjnej kary pieniężnej w niniejszym przypadku jest niezbędne zważywszy także na to, że Fundacja zignorowała fakt, iż z naruszeniem ochrony danych mamy do czynienia zarówno wówczas, gdy do zdarzenia dojdzie wskutek świadomego działania, jak i wtedy, gdy doprowadzi do niego nieumyślność.

W ocenie Prezesa UODO administracyjna kara pieniężna spełni funkcję represyjną, jako że stanowić będzie odpowiedź na naruszenie przez Fundację przepisów rozporządzenia 2016/679. Będzie ona również spełniać funkcję prewencyjną; w ocenie Prezesa UODO wskaże bowiem zarówno Fundacji, 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), zwanej dalej „u.o.d.o.", 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.

W związku z powyższym wskazać należy, że kara pieniężna w wysokości **13 644 PLN** (słownie: **trzynaście tysięcy sześćset czterdzieści cztery złote**), co stanowi równowartość 3 000 EUR (średni kurs euro z 28 stycznia 2021 r. - 4,5479 zł), 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 Fundacji administracyjnej kary pieniężnej, Prezes UODO uznał, iż jest ona proporcjonalna do sytuacji finansowej Fundacji i nie będzie stanowiła dla niej 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 powodujące konieczność istotnego ograniczenia pozytywnej z punktu widzenia interesu społecznego działalności Fundacji. Zdaniem Prezesa Urzędu Ochrony Danych Osobowych, Fundacja powinna i jest w stanie ponieść konsekwencje swoich zaniedbań w sferze ochrony danych, o czym świadczy chociażby przesłane do UODO w dniu [...] kwietnia 2021 r. sprawozdania finansowe Fundacji za okresy od [...] stycznia 2018 r. do [...] grudnia 2018 r., zgodnie z którym jej przychody z działalności statutowej wyniosły ok. 1 mln zł, oraz od [...] stycznia 2019 r. do [...] grudnia 2019 r., zgodnie z którym jej przychody z działalności statutowej wyniosły ok. 2,07 mln zł. Przedstawione przez Fundację dane finansowe obejmujące lata 2018-2019 (wskazujące na dużą dynamikę wzrostu przychodów, a tym samym rozwój działalności Fundacji) pozwalają przyjąć, że w 2020 r. czyli w poprzednim roku obrotowym przychody Fundacji (oparte w większości na środkach ze źródeł publicznych, w więc źródeł stabilnych) były nie niższe niż 2 mln zł. Przyjmując, na podstawie art. 101a ust. 2 u.o.d.o., taką wartość przychodów Fundacji jako podstawę wymiaru orzeczonej administracyjnej kary pieniężnej, Prezes UODO stwierdza, że kara w wysokości 13 644 zł nie będzie stanowić dla Fundacji nadmiernego obciążenia, będąc jednocześnie środkiem skutecznym i proporcjonalnym oraz działającym na przyszłość prewencyjnie - zarówno wobec Fundacji jak i innych podmiotów, na których spoczywają obowiązki określone w art. 33 ust. 1 i art. 34 ust. 1 rozporządzenia 2016/679.

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