PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Warszawa, dnia 05 stycznia 2021 r.

DECYZJA

DKE.561.11.2020

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2020 r., poz. 256 ze zm.), art. 7 ust. 1 i 2, art. 60, art. 101, art. 101a i art. 103 ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz art. 57 ust. 1 lit. a), art. 83 ust. 1-2 i art. 83 ust. 6 w związku z art. 58 ust. 2 lit. e) oraz lit. i) Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 1 z późn. zm.), po przeprowadzeniu wszczętego z urzędu postępowania administracyjnego w sprawie nałożenia na Panią M. Z. prowadzącą działalność gospodarczą pod firmą K. administracyjnej kary pieniężnej,Prezes Urzędu Ochrony Danych Osobowych,

stwierdzając niewykonanie przez Panią M. Z. prowadzącą działalność gospodarczą pod firmą K. nakazu decyzji administracyjnej Prezesa Urzędu Ochrony Danych Osobowych z dnia [...] lutego 2020 roku, (sygn. [...])

nakłada na Panią M. Z. prowadzącą działalność gospodarczą pod firmą K. administracyjną karę pieniężną w kwocie 85 588 PLN (słownie: osiemdziesiąt pięć tysięcy pięćset osiemdziesiąt osiem złotych).

UZASADNIENIE

Do Urzędu Ochrony Danych Osobowych wpłynęło zgłoszenie naruszenia ochrony danych osobowych z dnia [...] lipca 2019 roku złożone przez Panią M. Z. prowadzącą działalność gospodarczą pod firmą K., (zwaną dalej również „Przedsiębiorcą").W treści zgłoszenia Przedsiębiorca poinformował, że naruszenie polegało na nieuprawnionym skopiowaniu w dniu [...] kwietnia 2019 roku danych osobowych stu pacjentów z systemu ([A]) przychodni przez byłego pracownika celem wykorzystania ich do marketingu własnych usług. Jednocześnie wskazał, że naruszenie dotyczyło następujących kategorii danych osobowych pacjentów: numeru PESEL, imion

i nazwisk, imion rodziców, daty urodzenia, adresu zamieszkania lub pobytu oraz numeru telefonu. Przedsiębiorca zrezygnował z zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych, pomimo, że ocenił ryzyko naruszenia praw i wolności osób fizycznych za wysokie. W związku z powyższym Prezes Urzędu Ochrony Danych Osobowych (zwany dalej również „Prezesem UODO"), wystąpieniem z dnia [...] sierpnia 2019 roku (sygn. [...]), skierowanym do Przedsiębiorcy na podstawie art. 52 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781) oraz art. 34 ust. 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 (Dz. Urz. UE L 119 z 04.05.2016 r., str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018 r., str. 2) (zwanego dalej „Rozporządzeniem 2016/679"), wezwał go do niezwłocznego zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych oraz przekazania tym osobom zaleceń odnośnie zminimalizowania potencjalnych negatywnych skutków zaistniałego naruszenia. W wystąpieniu tym Prezes UODO wskazał ponadto Przedsiębiorcy przykładowe ryzyka związane z tego rodzaju naruszeniem oraz przykładowe zalecenia co do środków, jakie osoby dotknięte naruszeniem mogą podjąć celem zabezpieczenia się przed negatywnymi skutkami naruszenia.

W związku z brakiem reakcji Przedsiębiorcy na wystąpienie z dnia [...] sierpnia 2019 roku Prezes UODO wszczął postępowanie administracyjne w sprawie niezawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych. Decyzją administracyjną z dnia [...] lutego 2020 roku (sygn. [...]) Prezes UODO nakazał Przedsiębiorcy – na podstawie art. 58 ust. 2 lit. e) Rozporządzenia 2016/679 – zawiadomienie osób, których dane dotyczą – w terminie trzech dni od dnia, w którym decyzja stanie się ostateczna – o naruszeniu ochrony danych osobowych w celu przekazania im informacji wymaganych zgodnie z art. 34 ust. 2 Rozporządzenia 2016/679, tj.:

a) opisu charakteru naruszenia danych osobowych;

b) imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych osobowych 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 skutków.

Przedsiębiorca nie wniósł od wyżej wskazanej decyzji administracyjnej skargi do Wojewódzkiego Sądu Administracyjnego, w związku z czym stała się ona prawomocna z dniem [...] kwietnia 2020 roku.

Celem sprawdzenia, czy nałożone powyższą decyzją obowiązki zostały wykonane przez Przedsiębiorcę, Prezes UODO wszczął postępowanie sprawdzające o sygn. [...].

Pismem z dnia [...] maja 2020 roku wezwał Przedsiębiorcę do złożenia wyjaśnień i przedstawienia wykazu osób, którym przekazano informacje, o których mowa w nakazie decyzji, a także informacji o sposobie ich przekazania oraz dowodów na ich przekazanie (kopii dziesięciu przykładowych zawiadomień wraz z potwierdzeniem ich nadania). Pismem tym Przedsiębiorca pouczony został

jednocześnie, że stwierdzenie nieprzestrzegania nakazu nałożonego przez Prezesa UODO skutkować może nałożeniem na niego administracyjnej kary pieniężnej, zgodnie z art. 83 ust. 6 Rozporządzenia 2016/679. W odpowiedzi na powyższe wezwanie Przedsiębiorca nie przesłał żądanych kopii powiadomień, a jedynie pismem, które wpłynęło do Urzędu Ochrony Danych Osobowych dnia [...] maja 2020 r., jego pełnomocnik poinformował, że cyt. "Niestety mimo naszych chęci, nie byliśmy w stanie takiej listy stworzyć, gdyż nie wiemy których pacjentów dane zebrał lekarz, o którym mowa w zawiadomieniu złożonym przez K. Obecnie w naszych placówkach leczy się ponad [...] osób i powiadomienie wszystkich o możliwości naruszenia ich danych osobowych jest awykonalne".

W dniu [...] czerwca 2020 roku Prezes UODO skierował do Przedsiębiorcy upomnienie, o którym mowa w art. 15 § 1 ustawy z dna 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2020 r., poz. 1427 ze zm.), zawierające wezwanie Przedsiębiorcy do wykonania nakazu decyzji w terminie 7 dni i do udokumentowania wykonania tego nakazu poprzez przedstawienie dowodów w postaci wykazu osób, które zostały zawiadomione w związku z naruszeniem ochrony ich danych osobowych, zawierającego informację w jaki sposób zawiadomienie zostało przesłane, a także kopii wybranych dziesięciu pism wraz z potwierdzeniami nadania. Tego samego dnia pełnomocnik Przedsiębiorcy został również telefonicznie poinformowany o obowiązku wykonania nakazu decyzji Prezesa UODO i przedstawienia dowodów na jego wykonanie. Pismem, które wpłynęło do Urzędu Ochrony Danych Osobowych w dniu [...] czerwca 2020 r., pełnomocnik Przedsiębiorcy przedstawił kopie dziesięciu przesłanych listem poleconym w dniu [...] czerwca 2020 r. zawiadomień o treści cyt. „Informujemy, że w roku 2019 mogło dojść do naruszenia Pani/Pana danych osobowych (imię, nazwisko, nr telefonu) przez jednego z naszych lekarzy (D. B.). Jednocześnie informujemy, że ta osoba w naszej klinice już nie pracuje i toczy się przeciwko niemu postępowanie wyjaśniające. W razie pytań prosimy o kontakt z administratorem RODO w naszej placówce: M. K. [...]". Przedstawione kopie zawiadomień nie zawierały wszystkich informacji, do udzielenia których zobowiązany został Przedsiębiorca nakazem decyzji Prezesa UODO, tj. nie zawierały informacji dotyczących opisu charakteru naruszenia, opisu możliwych konsekwencji naruszenia oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu – w tym środków w celu zminimalizowania jego ewentualnych skutków. W związku z tym, pismem z dnia [...] lipca 2020 roku, Prezes UODO wezwał Przedsiębiorcę do uzupełnienia wyjaśnień oraz przedstawienia dowodów dokumentujących wykonanie decyzji. W odpowiedzi na ponowne wezwanie do złożenia wyjaśnień pełnomocnik Przedsiębiorcy wyjaśnił wiadomością e-mail z dnia [...] lipca 2020 roku, że cyt. „(...) punkty o których Pani wspomniała w wezwaniu zostały spełnione:

b) W razie pytań prosimy o kontakt z administratorem RODO w naszej placówce:

M. K. [...]

c) Nie da się tego punktu wyjaśnić, według mnie wystarczy jak wymieniliśmy jakie dane zostały naruszone.

d) Jednocześnie informujemy, że ta osoba w naszej klinice już nie pracuje i toczy się przeciwko niemu postępowanie wyjaśniające.

W związku z powyższym uważam, że nie ma podstawy do ponownego wysyłania zawiadomień do pacjentów."

W ocenie Prezesa UODO złożone przez pełnomocnika Przedsiębiorcy wyjaśnienia oraz przedstawione przez niego dowody dały podstawę do stwierdzenia, że Przedsiębiorca nie wykonał nakazu decyzji administracyjnej Prezesa UODO z [...] lutego 2020 roku, sygn.[...].

W związku z powyższym, pismem z dnia [...] września 2020 roku Prezes UODO wszczął z urzędu postępowanie administracyjne o sygn. DKE.561.11.2020.[..] w przedmiocie nałożenia na Przedsiębiorcę administracyjnej kary pieniężnej za nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lit. e) w związku z art. 34 ust. 1 i 2 Rozporządzenia 2016/679. Powyższym pismem Przedsiębiorca został m.in. wezwany do przedstawienia danych finansowych w postaci sprawozdania finansowego, a w razie jego braku – oświadczenia o wysokości obrotu i wyniku finansowego za 2019 roku, celem ustalenia podstawy wymiaru administracyjnej kary pieniężnej. Ponadto w piśmie tym wskazano, że jeżeli Przedsiębiorca przedstawi dowody na wykonanie w całości nakazu przedmiotowej decyzji Prezesa UODO, okoliczność ta może wpłynąć łagodząco na wymiar administracyjnej kary pieniężnej orzeczonej w niniejszym postępowaniu lub też może spowodować odstąpienie od jej nałożenia.

W odpowiedzi na pismo informujące o wszczęciu postępowania w przedmiocie nałożenia administracyjnej kary pieniężnej pełnomocnik Przedsiębiorcy wiadomością e-mail z dnia [...] września 2020 roku zobowiązał się do przesłania cyt. „ponownego powiadomienia dla pacjentów, których naruszenie dotyczyło". Ponadto w dniu [...] września 2020 roku pełnomocnik Przedsiębiorcy skontaktował się telefonicznie z Urzędem Ochrony Danych Osobowych prosząc o listę przedstawionych przez siebie wcześniej (pismem z dnia [...] czerwca 2020 roku) dziesięciu zawiadomień do sprawy o sygn. [...]. Został poinformowany, że w związku z obecnie prowadzonym wobec Przedsiębiorcy postępowaniem (sygn. DKE.561.11.2020.[..]) w przedmiocie nałożenie administracyjnej kary pieniężnej za nieprzestrzeganie nakazu orzeczonego przez Prezesa UODO decyzją sygn. [...], zobowiązany jest przedstawić kompletne zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony jej danych osobowych oraz listę wszystkich osób, których dotyczyło naruszenie wraz z potwierdzeniami wysłania zawiadomień, celem udokumentowania obowiązku wynikającego z nakazu decyzji. Na okoliczność tej rozmowy telefonicznej sporządzona została w dniu [...] września 2020 roku notatka służbowa. W dniu [...] września 2020 roku pełnomocnik Przedsiębiorcy wiadomością e-mail przesłał do Urzędu Ochrony Danych Osobowych przykładowe zawiadomienie, celem uzgodnienia jego treści z Urzędem a następnie przesłania osobom, których dotyczyło naruszenie ochrony danych osobowych. W związku z powyższą wiadomością e-mail, zawierającą przykładowe zawiadomienie o naruszeniu ochrony danych osobowych, pracownik UODO skontaktował się z pełnomocnikiem Przedsiębiorcy również drogą elektroniczną (w dniu [...] września 2020 roku), a następnie telefonicznie (w dniu [...] października 2020 roku), celem wyjaśnienia, że zawiadomienie jest niekompletne. Pełnomocnik Przedsiębiorcy został poinformowany, że zawiadomienie powinno wskazywać pełny (zgodny ze zgłoszeniem z dnia [...] lipca 2019 roku) zakres danych osobowych ujawnionych w wyniku naruszenia, a także powinno zawierać opis możliwych konsekwencji naruszenia ochrony danych osobowych i kroków zaradczych podjętych przez administratora. Pouczono pełnomocnika Przedsiębiorcy ponadto, że przykłady możliwych konsekwencji i kroków zaradczych zostały wskazane Przedsiębiorcy w treści decyzji

z dnia [...] lutego 2020 roku, sygn. [...]. Pełnomocnik Przedsiębiorcy w trakcie rozmowy telefonicznej zobowiązał się do przesłania dowodów wykonania nakazu zwartego w decyzji do końca miesiąca października 2020 roku. Pismem, które wpłynęło do Urzędu Ochrony Danych Osobowych w dniu [...] listopada 2020 roku, pełnomocnik Przedsiębiorcy oświadczył, że cyt. „Informuję, że zgodnie z wezwaniem przesłanym przez Departament Kar i Egzekucji Urzędu Ochrony Danych Osobowych, powiadomiliśmy łącznie 37 osób (poszkodowanych). Tyle osób ostatecznie wynikało z przeprowadzonej przez nasz dział informatyczny analizy logowań i informacji, które widział Pan D(...) B(...). Jednocześnie informuję, że są to wszystkie osoby poszkodowane w tej sprawie." W załączonej do pisma liście osób, którym Przedsiębiorca przesłał zawiadomienia o naruszeniu ich danych osobowych, wskazano trzydzieści siedem pozycji, przy czym dwie pozycje z listy powtórzyły się. Ponadto do pisma załączone zostały: kopia wystawionej przez Pocztę Polską S.A. na rzecz Przedsiębiorcy faktury VAT nr [...] z dnia [...] października 2020 roku dokumentującej zakup trzydziestu siedmiu znaczków pocztowych o wartości 3,30 zł każdy, kopia oświadczenia z dnia [...] października 2020 roku o treści „Potwierdzamy nadanie przez Pana M. K. listów zwykłych w ilości 37 sztuk" opatrzonego nieczytelnym podpisem i pieczęcią o treści „W. [...] *AN*" oraz kopia niezaadresowanego przykładowego zawiadomienia. W odpowiedzi na powyższe pismo, w dniu [...] listopada 2020 roku, Prezes UODO skierował do Przedsiębiorcy wezwanie do uzupełnienia dowodów wskazując, że przesłane wyjaśnienia oraz dowody są niekompletne i nie dają podstawy do stwierdzenia, że Przedsiębiorca istotnie powiadomił osoby, których dane dotyczą, zgodnie z nakazem decyzji administracyjnej Prezesa UODO z [...] lutego 2020 roku, sygn. [...]. Przedsiębiorca wezwany został do uzupełnienia dowodów wykonania nakazu decyzji, tj. do przesłania poprawnego wykazu osób, którym zostały przesłane zawiadomienia, oraz kopii wszystkich zaadresowanych zawiadomień wraz z potwierdzeniem nadania przesyłek poleconych lub zwrotnych potwierdzeń odbioru - w terminie 7 dni od dnia doręczenia niniejszego pisma. W odpowiedzi pełnomocnik Przedsiębiorcy pismem, które wpłynęło do UODO w dniu [...] grudnia 2020 roku, poinformował, że cyt. „nie ma obowiązku wysyłki listów poleconych i wystarczy, że wyślę je listem zwykłym i potwierdzę ich wysyłkę. Nakaz ten wykonałem i potwierdziłem to fakturą i zaświadczeniem pisemnym od pracownika poczty". Ponadto wskazał, że cyt. „ilość zawiadomień jest poprawna — powtórki pacjentów nie są przypadkowe, są wynikiem tego, że byli oni na wizycie dwukrotnie".

Po rozpatrzeniu całości materiału dowodowego zebranego w sprawie Prezes Urzędu Ochrony Danych Osobowych zważył, co następuje.

Stosownie do art. 57 ust. 1 Rozporządzenia 2016/679, bez uszczerbku dla innych zadań określonych na mocy tego rozporządzenia, każdy organ nadzorczy na swoim terytorium (w tym Prezes UODO na terytorium Rzeczypospolitej Polskiej) między innymi monitoruje i egzekwuje stosowanie rozporządzenia (art. 57 ust. 1 lit. a) oraz prowadzi postępowania w sprawie jego stosowania (art. 57 ust. 1 lit. h). Instrumentami realizacji zadań, o których mowa w art. 57 ust. 1 Rozporządzenia 2016/679, są uprawnienia naprawcze przyznane organom nadzorczym (w tym Prezesowi UODO) mocą art. 58 ust. 2 Rozporządzenia 2016/679, w tym w szczególności uprawnienie do nakazania administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych

osobowych (art. 58 ust. 2 lit. e), a także uprawnienie do zastosowania, oprócz lub zamiast innych środków, o których mowa w art. 58 ust. 2 Rozporządzenia 2016/679, administracyjnej kary pieniężnej na mocy art. 83 tego rozporządzenia (art. 58 ust. 2 lit. i).

Zgodnie z art. 83 ust. 6 Rozporządzenia 2016/679 nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 podlega administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Odnosząc wskazane wyżej przepisy Rozporządzenia 2016/679 do ustalonego w sprawie, a opisanego powyżej, stanu faktycznego stwierdzić należy, że Przedsiębiorca nie wykonał (czy też – zgodnie z terminologią użytą przez prawodawcę unijnego w art. 83 ust. 6 Rozporządzenia 2016/679) – „nie przestrzega”) nakazu decyzji administracyjnej Prezesa UODO z dnia [...] lutego 2020 roku, sygn. [...].

Prawomocną decyzją administracyjną Prezesa UODO z dnia [...] lutego 2020 roku, sygn. [...], Przedsiębiorca zobowiązany został do zawiadomienia osób, których dane dotyczą – w terminie trzech dni od dnia, w którym decyzja stanie się ostateczna – o naruszeniu ich danych osobowych, które miało miejsce w dniu [...] kwietnia 2019 roku, w celu przekazania im informacji wymaganych zgodnie z art. 34 ust. 2 Rozporządzenia 2016/679, tj.

a) opisu charakteru naruszenia danych osobowych;

b) imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych osobowych 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 skutków.

Prezes UODO wskazał w przedmiotowej decyzji administracyjnej, że właściwe wywiązanie się z obowiązku określonego w art. 34 Rozporządzenia 2016/679 ma zapewnić osobom, których dane dotyczą – szybko i w sposób przejrzysty – 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. Prezes UODO w uzasadnieniu decyzji podkreślił ponadto, że naruszenie poufności danych w postaci numeru PESEL wraz z imionami i nazwiskami, imionami rodziców, datą urodzenia, adresem zamieszkania lub pobytu oraz numerem telefonu powoduje wysokie ryzyko dla praw i wolności osób, których te dane dotyczą oraz wymaga zawiadomienia tych osób o naruszeniu celem poinformowania ich m.in. o możliwych negatywnych skutkach naruszenia oraz działaniach (środkach), jakie mogą one podjąć w celu zabezpieczenia przed negatywnymi skutkami naruszenia. Prezes UODO w konkluzji stwierdził, że postępując zgodnie z prawem i wykazując dbałość o interesy osób, których dane dotyczą, administrator (Przedsiębiorca) powinien był zatem bez zbędnej zwłoki zapewnić osobom, których dane dotyczą, możliwość jak najlepszej ochrony danych osobowych.

W ocenie Prezesa UODO Przedsiębiorca nie udowodnił – ani w trakcie postępowania sprawdzającego wykonanie decyzji Prezesa UODO (o sygn. […]), ani w trakcie niniejszego postępowania w przedmiocie nałożenia na Przedsiębiorcę administracyjnej kary pieniężnej (o sygn. DKE.561.11.2020.[…] – wykonania skierowanego do niego nakazu decyzji administracyjnej z dnia […] lutego 2020 roku, sygn. […].

Na wstępie podkreślić należy, że zgodnie ze sformułowaną w art. 5 ust. 2 Rozporządzenia 2016/679 zasadą rozliczalności administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 tego przepisu (w tym – zgodnie z tzw. zasadą legalności – za przetwarzanie danych osobowych „zgodnie z prawem") i musi być w stanie wykazać ich przestrzeganie. W niniejszej sprawie Prezes UODO prawomocnie stwierdził decyzją administracyjną z […] lutego 2020 roku, sygn. […], że Przedsiębiorca przetwarza dane osobowe niezgodnie z prawem, a konkretnie z przepisami art. 34 ust. 1 i 2 Rozporządzenia 2016/679 nakazującymi administratorowi – w przypadku wystąpienia naruszenia ochrony danych osobowych mogącego powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – bezzwłoczne zawiadomienie o tym naruszeniu (w formie i o treści określonymi w ust. 2) osób, których dane dotyczą. Zastosowanie zasady rozliczalności w niniejszej sprawie oznacza, że Przedsiębiorca zobowiązany jest – w szczególności w postępowaniu przed Prezesem UODO – udowodnić wykonanie nakazu decyzji, które to wykonanie byłoby równoznaczne z przywróceniem przetwarzania przez niego danych osobowych do stanu zgodnego z prawem. Takie implikacje zasady rozliczalności potwierdza doktryna prawa ochrony danych osobowych, zgodnie z którą „Stwierdzenie, że administrator powinien być w stanie wykazać przestrzeganie zasad, odczytywać można jako nałożenie na administratora ciężaru dowodowego w zakresie przestrzegania zasad przetwarzania danych. W razie sporu z osobą, której dane dotyczą, albo z organem nadzorczym, administrator powinien być w stanie przedstawić dowody na to, że przestrzega zasad. Dowodami takimi mogą być przede wszystkim dokumenty dotyczące przetwarzania i ochrony danych." (*P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 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) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, art. 5. https://sip.lex.pl/#/commentary/587773149/570589/fajgielski-pawel-komentarz-do-rozporzadze nia -nr-2016-679-w-sprawie-ochrony-osob-fizycznych-w…?cm=URELATIONS*).

W niniejszej sprawie – w ocenie Prezesa UODO – Przedsiębiorca nie przedstawił dowodów na wykonanie obowiązku, o którym mowa w art. 34 ust. 1 i 2 Rozporządzenia 2016/679.

Po pierwsze bowiem, Przedsiębiorca udowodnił (przedstawiając kopię pocztowej książki nadawczej) skierowanie w dniu […] czerwca 2020 roku zawiadomień o naruszeniu ochrony danych osobowych do dziesięciu osób. Wobec treści tych zawiadomień – bezsprzecznie nieodpowiadających wymogom art. 34 ust. 2 Rozporządzenia 2016/679 – oraz niewielkiej ich liczby w stosunku do wskazanej w zgłoszeniu z dnia […] lipca 2019 roku liczby stu osób, których dane naruszono (czy też liczby trzydziestu siedmiu osób wskazanej przez Przedsiębiorcę - po sprawdzeniu – w piśmie, które wpłynęło do Urzędu Ochrony Danych Osobowych w dniu […] listopada 2020 r.), działania tego w żaden sposób nie można uznać za wykonanie nakazu decyzji Prezesa UODO.

Po drugie zaś, dokumenty przedstawione przez Przedsiębiorcę jako dowód skierowania w dniu [...] lub [...] października 2020 r. zawiadomień do trzydziestu siedmiu osób nie wskazują jednoznacznie, że takie zawiadomienia rzeczywiści zostały skierowane do osób, których dane naruszono. Świadczą o tym następujące okoliczności:

a) Faktura VAT nr [...] z dnia [...] października 2020 roku dokumentuje jedynie zakup trzydziestu siedmiu znaczków pocztowych a nie wykonanie usługi pocztowej (doręczenie przesyłki pocztowej).

b) Brak jest pewności, że oświadczenie o treści „Potwierdzamy nadanie przez Pana M. K. listów zwykłych w ilości 37 sztuk" pochodzi od operatora pocztowego (brak jest wskazania firmy operatora lub jakiegokolwiek innego jego oznaczenia). Oświadczenie to jest ponadto nieweryfikowalne i w związku z tym niewiarygodne – ze względu na nieczytelny podpis nie można bowiem zidentyfikować osoby składającej to oświadczenie.

c) Nawet gdyby powyższe oświadczenie potwierdzało fakt wysłania przez Przedsiębiorcę trzydziestu siedmiu listów zwykłych (co jak wskazano wyżej nie zachodzi) to z całą pewnością nie można w oparciu o nie (nawet biorąc pod uwagę również fakturę dokumentującą zakup znaczków pocztowych) stwierdzić, że były to zawiadomienia, o których mowa w nakazie decyzji, że zawierały treść zgodną z przedstawionym przez Przedsiębiorcę przykładowym (niezaadresowanym) zawiadomieniem, i ostatecznie - że zostały skierowane do osób dotkniętych naruszeniem (wymienionym w sporządzonym przez Przedsiębiorcę wykazie).

Podsumowując powyższe stwierdzić należy, że brak jest podstaw do uznania, że Przedsiębiorca wywiązał się z ciążącego na nim na mocy art. 34 ust 1 i 2 Rozporządzenia 2016/679 obowiązku zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych, będącym przedmiotem zgłoszenia z dnia [...] lipca 2019 roku, i tym samym wykonał nakaz decyzji administracyjnej Prezesa UODO z dnia [...] lutego 2020 roku, sygn. [...]. Stan nieprzestrzegania nakazu orzeczonego przez Prezesa UODO jest aktualny na dzień wydania niniejszej decyzji.

W tym miejscu wskazać należy, że stan naruszenia przepisów Rozporządzenia 2016/679 stanowiącego przedmiot niniejszego postępowania, to jest nieprzestrzegania nakazu orzeczonego przez Prezesa UODO, trwa od dnia [...] marca 2020 r., to jest od dnia następującego po dniu, w którym upłynął wyznaczony w decyzji termin na jego wykonanie. Podkreślić natomiast trzeba, że stan naruszenia przepisów Rozporządzenia 2016/679, którego usunięciu służyć miał nakaz decyzji (stan niepoinformowania o naruszeniu osób, których to naruszenie dotyczy), jest zdecydowanie dłuższy; trwa co najmniej od [...] lipca 2019 r. kiedy to Przedsiębiorca dokonał zgłoszenia naruszenia ochrony danych osobowych, miał więc już o nim niewątpliwie wiedzę.

Przedsiębiorca, pomimo prawidłowego doręczenia mu decyzji Prezesa UODO, w żaden sposób nie próbował wykonać orzeczonego nakazu. Jakiekolwiek działania podjął dopiero na skutek interwencji Prezesa UODO. Działania te były jednak opieszałe i – jak to wykazano wyżej – nieskuteczne, co zwiększyło ryzyko wystąpienia po stronie osób dotkniętych naruszeniem dodatkowych szkód. Zgodnie z motywem 86 Rozporządzenia 2016/679 „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. Na przykład potrzeba zminimalizowania

bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie".

Podkreślić należy, że zarówno w trakcie postępowania sprawdzającego wykonanie decyzji Prezesa UODO (o sygn. [...]) jak i w trakcie niniejszego postępowania w przedmiocie nałożenia na Przedsiębiorcę administracyjnej kary pieniężnej (o sygn. DKE.561.11.2020.[...]) pracownik UODO udzielił Przedsiębiorcy szeregu wskazówek dotyczących wykonania nakazu, w szczególności dotyczących prawidłowego sformułowania zawiadomień i formy ich przekazania osobom zainteresowanym, a także sposobu udokumentowania tych czynności przed Prezesem UODO odpowiedzialnym za wyegzekwowanie orzeczonych przez siebie nakazów. Niezastosowanie się przez Przedsiębiorcę do tych wskazówek, a wręcz ich ignorowanie, świadczy w ocenie Prezesa UODO o rażącym lekceważeniu przez niego obowiązków związanych z ochroną danych osobowych.

Mając na uwadze powyższe rozważania, Prezes UODO stwierdza, że w niniejszej sprawie zaistniały przesłanki uzasadniające nałożenie na Przedsiębiorcę - na mocy art. 83 ust. 6 Rozporządzenia 2016/679 - administracyjnej kary pieniężnej w związku z nieprzestrzeganiem nakazu orzeczonego na podstawie art. 58 ust. 2 lit. e) Rozporządzenia 2016/679. Stosownie do treści art. 83 ust. 2 Rozporządzenia 2016/679 administracyjne kary pieniężne nakłada się zależnie od okoliczności każdego indywidualnego przypadku. Zwraca się przy tym w każdym przypadku na szereg okoliczności wymienionych w punktach od a) do k) wskazanego wyżej przepisu. Decydując o nałożeniu w niniejszej sprawie na Przedsiębiorcę administracyjnej kary pieniężnej oraz ustalając jej wysokość, Prezes UODO wziął - spośród nich - pod uwagę następujące okoliczności wpływające obciążająco na ocenę naruszenia:

a) Charakter, waga i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania (art. 83 ust. 2 lit. a) Rozporządzenia 2016/679)

Naruszenie podlegające administracyjnej karze pieniężnej w niniejszym postępowaniu (nieprzestrzeganie nakazu orzeczonego przez Prezesa UODO na podstawie art. 58 ust. 2 Rozporządzenia 2016/679) godzi w system mający na celu ochronę jednego z podstawowych praw osoby fizycznej, którym jest prawo do ochrony jej danych osobowych, czy też szerzej - do ochrony jej prywatności. Istotnym elementem tego systemu, którego ramy określone zostały Rozporządzeniem 2016/679, są organy nadzorcze, na które nałożone zostały zadania związane z ochroną i egzekwowaniem praw osób fizycznych w tym zakresie. W celu umożliwienia realizacji tych zadań organy nadzorcze wyposażone zostały w szereg uprawnień naprawczych, w tym w uprawnienie do nakazania administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych (art. 58 ust. 2 lit. e). Lekceważenie przez Przedsiębiorcę orzeczonego wobec niego przez Prezesa UODO nakazu, będącego w istocie skonkretyzowaniem obowiązku przewidzianego przepisami Rozporządzenia 2016/679, oznacza w istocie lekceważenie przepisów o ochronie danych osobowych i roli Prezesa UODO w systemie ochrony danych określonym przepisami Rozporządzenia 2016/679. Takie postępowanie Przedsiębiorcy będącego podmiotem profesjonalnie i na dużą skalę przetwarzającego dane osobowe pacjentów (w tym dane dotyczące zdrowia, a więc dane podlegające szczególnej ochronie na mocy art. 9 Rozporządzenia 2016/679)

uznać należy za mające dużą wagę i za szczególnie naganne. Wagę naruszenia zwiększa dodatkowo okoliczność, że dokonane przez Przedsiębiorcę naruszenie nie było zdarzeniem jednorazowym i incydentalnym; postępowanie Przedsiębiorcy podlegające ocenie w niniejszym postępowaniu ma charakter ciągły i długotrwały. Trwa od dnia [...] marca 2020 r., to jest od dnia następującego po dniu, w którym upłynął wyznaczony w decyzji termin na wykonanie nakazu zawartego w decyzji, do chwili obecnej. Tak długi czas trwania naruszenia (wydłużający stan naruszenia przepisu art. 34 Rozporządzenia 2016/679, którego usunięciu służyć miał nakaz decyzji, co zwiększa niewątpliwie ryzyko zaistnienia negatywnych konsekwencji dla osób dotkniętych naruszeniem) sprzeczny jest z ratio legis przepisu art. 34 Rozporządzenia 2016/679 zakładającego, że dla zminimalizowania ryzyka powstania szkód po stronie osób dotkniętych naruszeniem, zawiadomienie o naruszeniu ich danych osobowych powinno nastąpić jak najszybciej – „bez zbędnej zwłoki" (art. 34 ust. 1 Rozporządzenia 2016/67/679). Wagę naruszenia przez administratora tego obowiązku podkreślono m.in. w Wytycznych WP 253 Grupy Roboczej Art. 29 z dnia 3 października 2017 roku w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów Rozporządzenia 2016/679 (*https://uodo.gov.pl/pl/10/13*), zgodnie z którymi „administrator/podmiot przetwarzający, który wykazał się niedbałością, gdyż nie dopełnił obowiązku powiadomienia lub co najmniej nie powiadomił o wszystkich szczegółach naruszenia wskutek niepoprawnej oceny rozmiaru naruszenia, może według organu nadzorczego zasłużyć na poważniejszą sankcję – innymi słowy jest mało prawdopodobne, by takie naruszenie zostało uznane za niewielkie".

b) Umyślny charakter naruszenia (art. 83 ust. 2 lit. b) Rozporządzenia 2016/679)

Grupa Robocza Art. 29 w wytycznych w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów Rozporządzenia 2016/679 przyjętych 3 października 2017 r. odnosząc się do umyślnego lub nieumyślnego charakteru naruszenia wskazała, że zasadniczo „umyślność" obejmuje zarówno wiedzę, jak i celowe działanie, w związku z cechami charakterystycznymi czynu zabronionego, podczas gdy „nieumyślność" oznacza brak zamiaru spowodowania naruszenia, pomimo niedopełnienia przez administratora albo podmiot przetwarzający wymaganego prawem obowiązku staranności. Umyślne naruszenia są poważniejsze niż te nieumyślne, a w konsekwencji częściej wiążą się z nałożeniem administracyjnej kary pieniężnej. Przedsiębiorca w toku postępowania ignorował zalecenia Urzędu co do poprawnego wykonania ciążącego na nim obowiązku, co wskazuje na celowe nieprzestrzeganie nakazu. Podkreślić należy, że na żadnym etapie postępowania Przedsiębiorca nie przedstawił kompletnych dowodów na wykonanie nakazu ww. decyzji.

c) Niezadowalający stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków (art. 83 ust. 2 lit. f) Rozporządzenia 2016/679)

Oceniając współpracę Przedsiębiorcy z Prezesem UODO w toku całej sprawy zainicjowanej zgłoszeniem przez niego w dniu [...] lipca 2019 roku naruszenia ochrony danych osobowych, stwierdzić należy, że jeszcze przed zaistnieniem naruszenia, to jest przed datą [...] marca 2020 r. (datą upływu terminu wykonania nakazu decyzji Prezesa UODO z dnia 26 lutego 2020 roku, sygn. [...]) Przedsiębiorca zlekceważył całkowicie zastosowane wobec niego przez Prezesa UODO środki – zarówno wystąpienie Prezesa UODO z dnia [...] sierpnia 2019 roku (sygn. [...]) jak i samą decyzję

Prezesa UODO z dnia [...] lutego 2020 roku. Pomimo prawidłowego doręczenia Przedsiębiorcy obu dokumentów, nie podjął on żadnych działań celem ich wykonania. Dopiero po wszczęciu przez Prezesa UODO postępowania sprawdzającego wykonanie decyzji (o sygn. [...]), jak również w trakcie niniejszego postępowania w przedmiocie nałożenia na niego administracyjnej kary pieniężnej (o sygn. DKE.561.11.2020.[...]), Przedsiębiorca nawiązał korespondencję z Prezesem UODO oraz podjął pewne działania w celu wykonania nakazu decyzji. Jak wykazano to wyżej, działania te były jednak opieszałe i nieskuteczne; nie zakończyły się – pomimo odpowiednich wskazówek udzielanych pełnomocnikowi Przedsiębiorcy przez pracownika UODO pisemnie, drogą elektroniczną i telefonicznie – wykonaniem przez Przedsiębiorcę obowiązku, o którym mowa w art. 34 Rozporządzenia 2016/679, oraz wykazaniem tego faktu przed Prezesem UODO.

Pozostałe przesłanki wymiaru administracyjnej kary pieniężnej wskazane w art. 83. ust. 2 Rozporządzenia 2016/679 nie miały wpływu (obciążającego lub łagodzącego) na dokonaną przez Prezesa UODO ocenę naruszenia (w tym: stopień odpowiedzialności administratora z uwzględnieniem wdrożonych środków technicznych i organizacyjnych, wszelkie stosowne wcześniejsze naruszenia ze strony administratora, kategorie danych osobowych, których dotyczyło naruszenie, sposób w jaki organ nadzorczy dowiedział się o naruszeniu, przestrzeganie zastosowanych w tej samej sprawie środków, o których mowa w art. 58 ust. 2 Rozporządzenia 2016/679, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, osiągnięte w związku z naruszeniem korzyści finansowe lub uniknięte straty).

Stosownie do brzmienia art. 83 ust. 1 Rozporządzenia 2016/679 nałożona przez organ nadzorczy administracyjna kara pieniężna powinna być w każdym indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca. W ocenie Prezesa UODO kara nałożona na Przedsiębiorcę w niniejszym postępowaniu spełnia te kryteria. Dolegliwość kary zdyscyplinuje Przedsiębiorcę do przestrzegania nakazów decyzji oraz do prawidłowej współpracy z Prezesem UODO w ewentualnych innych postępowaniach prowadzonych w przyszłości z udziałem Przedsiębiorcy. Nałożona niniejszą decyzją kara jest – w ocenie Prezesa UODO – proporcjonalna do dużej wagi i nagannego charakteru stwierdzonego naruszenia. Kara ta spełni ponadto funkcję odstraszającą; będzie jasnym sygnałem zarówno dla Przedsiębiorcy jak i dla innych adresatów decyzji Prezesa UODO, że nieprzestrzeganie orzeczonego przez niego nakazu stanowi odrębne (niezależne od naruszenia, którego usunięcie leżało u podstaw orzeczonego nakazu) naruszenie, i to naruszenie o znacznej wadze. Jako takie podlegać będzie więc sankcjom finansowym. W tym miejscu wskazać należy, że w ocenie Prezesa UODO nałożenie na Przedsiębiorcę administracyjnej kary pieniężnej jest środkiem, który zapewni przestrzeganie nakazu orzeczonego wobec niego w drodze decyzji z dnia [...] lutego 2020 roku o sygn.[...].

Wobec nieprzedstawienia przez Przedsiębiorcę żądanych przez Prezesa UODO danych finansowych za rok 2019, ustalając wysokość administracyjnej kary pieniężnej w niniejszej sprawie wzięto pod uwagę szacunkową wielkość przedsiębiorstwa Przedsiębiorcy oraz specyfikę, zakres i skalę jego działalności. W trakcie postępowania ustalono, że Przedsiębiorca prowadzi działalność gospodarczą na dużą skalę w sektorze usług generującym niewątpliwie duże przychody i zyski, to jest w ochronie zdrowia. Z informacji przedstawionych na stronie internetowej Przedsiębiorcy ([...]) wynika, że

prowadzi on co najmniej trzy placówki medyczne: D., K. oraz K.. Dużą skalę działalności Przedsiębiorcy potwierdził sam pełnomocnik Przedsiębiorcy w piśmie, które wpłynęło do Urzędu Ochrony Danych Osobowych dnia [...] maja 2020 r., w którym stwierdził cyt. „Obecnie w naszych placówkach leczy się ponad [...] osób." Wobec powyższego stwierdzić należy, że orzeczona w niniejszej decyzji administracyjna kara pieniężna nie będzie wiązać się z nadmiernym dla prowadzonej przez Przedsiębiorcę działalności uszczerbkiem.

Zgodnie z brzmieniem 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. W niniejszej sprawie zastosowanie ma kurs 4,2794 zł za 1 EUR obowiązujący w dniu 28 stycznia 2020 r. Orzeczona niniejszą decyzją administracyjna kara pieniężna w wysokości 85 588 złotych stanowi więc równowartość 20 000 EUR.

Mając powyższe na uwadze Prezes UODO orzekł jak w sentencji niniejszej decyzji.

Decyzja jest ostateczna. Od decyzji stronie przysługuje prawo wniesienia skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie, w terminie 30 dni od dnia jej doręczenia, za pośrednictwem Prezesa UODO (adres: ul. Stawki 2, 00 - 193 Warszawa). Od skargi należy wnieść wpis stosunkowy, zgodnie z art. 231 w związku z art. 233 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2019 r., poz. 2325). Zgodnie z art. 74 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781) wniesienie przez stronę skargi do sądu administracyjnego wstrzymuje wykonanie decyzji w zakresie administracyjnej kary pieniężnej.

Zgodnie z art. 105 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781), administracyjną karę pieniężną należy uiścić w terminie 14 dni od dnia upływu terminu na wniesienie skargi do Wojewódzkiego Sądu Administracyjnego, albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego, na rachunek bankowy Urzędu Ochrony Danych Osobowych w NBP O/O Warszawa nr 28 1010 1010 0028 8622 3100 0000. Ponadto, zgodnie z art. 105 ust. 2 wskazanej wyżej ustawy Prezes UODO może, na uzasadniony wniosek podmiotu ukaranego, odroczyć termin uiszczenia administracyjnej kary pieniężnej albo rozłożyć ją na raty. W przypadku odroczenia terminu uiszczenia administracyjnej kary pieniężnej albo rozłożenia jej na raty, Prezes UODO nalicza od nieuiszczonej kwoty odsetki w stosunku rocznym, przy zastosowaniu obniżonej stawki odsetek za zwłokę, ogłaszanej na podstawie art. 56d ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2019 r. poz. 900, z późn. zm.), od dnia następującego po dniu złożenia wniosku.