PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Warszawa, dnia 20 grudnia 2023 r.

Decyzja
DKN.5131.32.2023

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2023 r. poz. 775 ze zm.) w związku z art. 7, art. 60, art. 102 ust. 1 pkt 1 i ust. 3 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz art. 57 ust. 1 lit. a) i lit. h), art. 58 ust. 2 lit. d), e) i lit. i), art. 83 ust. 1 i 2, art. 83 ust. 4 lit. a) w związku z art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 i 2 oraz art. 34 ust. 2 i 4 w związku z art. 33 ust. 3, a także art. 83 ust. 5 lit. a) w związku z art. 5 ust. 1 lit. a) i f), art. 5 ust. 2, art. 6 ust. 1 i art. 9 ust. 1 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 rozporządzenia 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), po przeprowadzeniu wszczętego z urzędu postępowania administracyjnego w sprawie naruszenia przepisów o ochronie danych osobowych przez Ministra Zdrowia (Warszawa, ul. Miodowa 15), Prezes Urzędu Ochrony Danych Osobowych,

stwierdzając naruszenie przez Ministra Zdrowia (Warszawa, ul. Miodowa 15) przepisów: a) art. 6 ust. 1 oraz art. 9 ust. 1 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", polegające na niezgodnym z prawem przetwarzaniu danych osobowych, w tym danych szczególnej kategorii, poprzez ich pozyskanie z Elektronicznej Platformy [...], o której mowa w art. 7 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465), oraz opublikowanie na platformie społecznościowej X (dawniej Twitter) bez podstawy prawnej, co skutkowało naruszeniem zasad zgodności z prawem, rzetelności i przejrzystości, określonej w art. 5 ust. 1 lit. a) rozporządzenia 2016/679), zasady integralności i poufności, wyrażonej

w art. 5 ust. 1 lit. f) rozporządzenia 2016/679 oraz zasady rozliczalności, o której mowa w art. 5 ust. 2 rozporządzenia 2016/679;

b) art. 24 ust. 1, art. 25 ust 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679, polegające na niewdrożeniu odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych przy wykorzystaniu Elektronicznej Platformy [...], o której mowa w art. 7 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465), w tym ich ochrony przed przypadkową utratą, zniszczeniem lub uszkodzeniem oraz ujawnieniem osobom nieuprawnionym,
co skutkowało naruszeniem zasad integralności i poufności (art. 5 ust. 1 lit. f) rozporządzenia 2016/679) oraz zasady rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679);

c) art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679, polegające na nieprzedstawieniu osobie, której dane naruszono w sposób określony w pkt. a), informacji, o których mowa w art. 33 ust. 3 lit. c) i d) rozporządzenia 2016/679, to jest opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym środków w celu zminimalizowania jego ewentualnych negatywnych skutków;

1) nakłada na Ministra Zdrowia (Warszawa, ul. Miodowa 15) za naruszenie art. 5 ust. 1 lit. a) i f), art. 5 ust. 2, art. 6 ust. 1, art. 9 ust. 1, art. 25 ust. 1, art. 32 ust. 1 i 2 oraz art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679 administracyjną karę pieniężną w kwocie 100 000 zł (słownie: stu tysięcy złotych);

2) nakazuje Ministrowi Zdrowia (Warszawa, ul. Miodowa 15) wdrożenie – w terminie 30 dni od dnia doręczenia niniejszej decyzji – odpowiednich środków technicznych i organizacyjnych w celu zminimalizowania ryzyka wiążącego się z przetwarzaniem danych osobowych przy wykorzystaniu Elektronicznej Platformy [...], o której mowa w art. 7 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465), w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, po uprzednim przeprowadzeniu analizy ryzyka, uwzględniającej stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych;

3) nakazuje Ministrowi Zdrowia (Warszawa, ul. Miodowa 15) zawiadomienie - w terminie 3 dni od dnia doręczenia niniejszej decyzji - osoby, której dane zostały ujawnione na platformie społecznościowej X (dawniej Twitter), o naruszeniu ochrony danych osobowych w celu

przekazania jej informacji określonych w art. 34 ust. 2 w związku z art. 33 ust. 3 lit. c) i d) rozporządzenia 2016/679, tj.:
-opisu możliwych konsekwencji naruszenia ochrony danych osobowych;
-opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Uzasadnienie

Minister Zdrowia (dalej także Administrator) w dniu 4 sierpnia 2023 r. opublikował w serwisie społecznościowym X (dawniej Twitter) wpis zawierający informację na temat lekarza, który wystawił receptę „pro auctore" na lek z grupy psychotropowych i przeciwbólowych, którego dotyczy rozporządzenie Ministra Zdrowia z dnia 12 lipca 2023 r. zmieniające rozporządzenie w sprawie środków odurzających, substancji psychotropowych, prekursorów kategorii 1 i preparatów zawierających te środki lub substancje (Dz. U. z 2023 r. poz. 1368). We wpisie znalazły się dane osobowe lekarza w postaci imienia i nazwiska, miejsca pracy oraz informacji o kategorii leku, na który została wystawiona recepta. W związku z ww. wydarzeniem, w dniu 9 sierpnia 2023 r. do Prezesa Urzędu Ochrony Danych Osobowych, dalej Prezes UODO, wpłynęło wstępne zgłoszenie naruszenia ochrony danych osobowych dokonane przez Ministra Zdrowia, w którym wskazano na wystąpienie naruszenia ochrony danych osobowych przetwarzanych przy wykorzystaniu Elektronicznej Platformy […], o której mowa w art. 7 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465), zwanej dalej również „systemem […]". W zgłoszeniu Administrator potwierdził fakt uzyskania przez Ministra Zdrowia danych osobowych lekarza z systemu […] za pomocą osób upoważnionych do korzystania z ww. systemu. Wskazano, iż Dyrektor Pionu […] w Ministerstwie Zdrowia, na ustne polecenie Ministra Zdrowia, wyznaczył pracownika, który odszyfrował w systemie […] receptę, na której znajdowały się dane osobowe lekarza, a następnie przekazał informacje, które się na niej znajdowały, Ministrowi Zdrowia.

W dniu 8 września 2023 r. do Urzędu Ochrony Danych Osobowych wpłynęło zgłoszenie uzupełniające naruszenia ochrony danych osobowych, w którym Administrator zamieścił brakującą w zgłoszeniu wstępnym treść zawiadomienia o naruszeniu ochrony danych osobowych skierowanego do osoby, której dane dotyczą. W zawiadomieniu skierowanym do lekarza brakowało jednak wszystkich informacji określonych w art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679, tj. opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu – w tym w stosownych przypadkach – środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Wobec powyższego, pismami z dni 9 sierpnia 2023 r. oraz 13 września 2023 r. Prezes UODO zwrócił się do Ministra Zdrowia o udzielenie odpowiedzi na pytania dotyczące:

a) podstawy prawnej uzyskania przez Ministra Zdrowia dostępu do danych o wystawieniu przez lekarza e-recepty na leki z grupy psychotropowych i przeciwbólowych oraz udostępnienia ich za pośrednictwem portalu społecznościowego X (dawniej: Twitter);
b) czy zostały opracowane i wdrożone zasady i procedury nadawania uprawnień w ww. systemie oraz w jaki sposób monitorowane było ich przestrzeganie;
c) czy Administrator przeprowadził analizę ryzyka w związku z przetwarzaniem danych osobowych związanych z wystawionymi e-receptami za pośrednictwem systemu [...];
d) czy analiza ta uwzględnia zagrożenia związane z nieuprawnionym uzyskaniem dostępu do tych danych, jak również wykazanie rozliczalności systemu [...].

Jednocześnie Prezes UODO zwrócił się o wyjaśnienie, za pomocą jakiego kanału komunikacji dane osobowe lekarza zostały przekazane Ministrowi Zdrowia z systemu [...] oraz w jaki sposób zostały one zabezpieczone, a także wskazanie ogólnego opisu technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych przez Administratora, środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osoby, której dane dotyczą, jakie działania planuje podjąć Administrator w celu wyeliminowania ryzyka wystąpienia analogicznych zdarzeń w przyszłości wraz ze wskazaniem terminu ich realizacji. Ponadto, Prezes UODO zwrócił się o ponowne, prawidłowe zawiadomienie osoby, której dane dotyczą, z uwagi na nieprzekazanie jej wszystkich wymaganych stosownie do art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679 informacji.

W odpowiedziach z dni 16 sierpnia 2023 r., 27 września 2023 r. oraz 13 października 2023 r. Administrator wskazał ogólny cel przetwarzania danych osobowych znajdujących się w systemie [...] oraz zaznaczył, że *„publikacja danych pochodzących z systemu [...] nie miała podstaw w przepisach prawa powszechnie obowiązującego”*, przedstawił procedurę nadawania uprawnień w systemie [...] wraz z informacją o osobach upoważnionych do korzystania z systemu, jak również przedstawił analizę ryzyka (bez daty) dla przetwarzania danych osobowych za pomocą systemu [...]. Ponadto, przedstawił środki bezpieczeństwa, o które zwrócił się Prezes UODO wraz z datą realizacji oraz wskazał, iż dane osobowe lekarza pozyskane z systemu [...] zostały przekazane Ministrowi Zdrowia za pośrednictwem komunikatora Whatsapp. Administrator przedstawił także treść ponownego zawiadomienia skierowanego do osoby, której dane dotyczą.

W związku ze zgłoszonym naruszeniem ochrony danych osobowych oraz wyjaśnieniami złożonymi przez Administratora ww. pismami, Prezes UODO w dniu 18 października 2023 r. wszczął z urzędu postępowanie administracyjne w zakresie możliwości naruszenia przez Ministra Zdrowia, jako administratora danych, przepisów art. 5 ust. 1 lit. a) i f), art. 5 ust. 2, art. 6 ust. 1, art. 9 ust. 1, art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 i 2 oraz art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679, w związku z naruszeniem ochrony danych osobowych lekarza poprzez ujawnienie na platformie społecznościowej X (dawniej Twitter) informacji przetwarzanych przez Administratora w systemie [...] (sygn. pisma DKN.5131.32.2023.).

W dniu 1 grudnia 2023 r, w celu uzupełnienia materiału dowodowego, Prezes UODO zwrócił się do Ministra Zdrowia o wyjaśnienie, czy opracowana została procedura zatytułowana „[...]", oraz czy zakończone zostały audyty Ministerstwa Zdrowia i C. wraz z przekazaniem dat ich zakończenia oraz przedstawieniem stosownych raportów. Ponadto, Prezes UODO zwrócił się o wskazanie, czy przed wystąpieniem naruszenia ochrony danych osobowych Administrator posiadał opracowane i wdrożone procedury określające zasady i tryb przekazywania danych osobowych, w tym danych z systemu [...], pomiędzy Ministerstwem Zdrowia a C. oraz przekazywanie tych danych osobowych pomiędzy poszczególnymi komórkami organizacyjnymi Ministerstwa Zdrowia.

W odpowiedzi z dnia 6 grudnia 2023 r. Administrator przekazał informację o etapie prac nad wprowadzeniem ww. procedury, przedstawił daty zakończenia audytów wraz z raportami oraz przedstawił procedury obowiązujące przed wystąpieniem naruszenia ochrony danych, tj. procedurę pn. „[...]" obowiązującą w C. oraz procedury dotyczące nadawania i odbierania uprawnień obowiązujące w Ministerstwie Zdrowia.

Organ nadzorczy dokonał oceny materiału dowodowego pod kątem zbadania jego wiarygodności i mocy dowodowej. Prezes UODO uznał przedłożone przez Administratora dowody za wiarygodne. Za powyższym przemawia fakt, że wyjaśnienia Ministra Zdrowia są logiczne, spójne i korelują z całością materiału dowodowego oraz potwierdzone zostały szeregiem dokumentów dostarczonych przez Administratora.

W tym stanie faktycznym, po zapoznaniu się z całością zgromadzonego w sprawie materiału dowodowego, Prezes Urzędu Ochrony Danych Osobowych zważył, co następuje:

Art. 5 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465) wskazuje, iż system informacji w ochronie zdrowia obejmuje bazy danych funkcjonujące w ramach Systemu [...], dziedzinowych systemów teleinformatycznych oraz rejestrów medycznych. Art. 5 ust. 2 ww. ustawy określa, że system informacji jest obsługiwany przez Platformę [...] oraz Elektroniczną Platformę [...], tj. system [...].

Art. 7 ust. 1 pkt 8 ustawy o systemie informacji w ochronie zdrowia wskazuje, że Elektroniczna Platforma [...] (system [...]) jest systemem teleinformatycznym, który umożliwia w szczególności dostęp ministra właściwego do spraw zdrowia do danych niezbędnych do realizacji zadań określonych w art. 11 ust. 1 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2022 poz. 2561 ze zm.).

Z kolei art. 11 ust. 1 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych stanowi, że do zadań ministra właściwego do spraw zdrowia w zakresie objętym ustawą należy w szczególności:
1) prowadzenie oraz współuczestniczenie w prowadzeniu edukacji w zakresie zapobiegania

i rozwiązywania problemów związanych z negatywnym wpływem na zdrowie czynników środowiskowych i społecznych;
1a) prowadzenie działań oraz współuczestniczenie w działaniach związanych z promocją zdrowia i profilaktyką chorób, w tym w ramach programów polityki zdrowotnej, o których mowa w art. 48, oraz programów wieloletnich ustanowionych na podstawie art. 136 ust. 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r. poz. 1634, ze zm.);
1b) ustalanie programów pilotażowych, o których mowa w art. 48e;
2) *(uchylony)*;
3) opracowywanie, finansowanie i ocena efektów programów polityki zdrowotnej, a także nadzór nad ich realizacją;
3a) kwalifikowanie świadczeń opieki zdrowotnej jako świadczeń gwarantowanych;
3b) zatwierdzanie oraz zmiana taryfy świadczeń;
4) finansowanie z budżetu państwa, z części pozostającej w dyspozycji ministra właściwego do spraw zdrowia, świadczeń gwarantowanych w zakresie określonym w ustawie, w tym w stosunku do osób uprawnionych do świadczeń opieki zdrowotnej na podstawie przepisów o koordynacji;
4a) planowanie, przekazywanie i rozliczanie dotacji z budżetu państwa, o której mowa w art. 97 ust. 8;
5) współdziałanie z organizacjami pozarządowymi o charakterze regionalnym lub ogólnokrajowym działającymi na rzecz ochrony zdrowia;
6) sprawowanie nadzoru nad ubezpieczeniem zdrowotnym w zakresie określonym w dziale VII;
7) zatwierdzanie planu finansowego Funduszu w porozumieniu z ministrem właściwym do spraw finansów publicznych;
8) opiniowanie sprawozdania finansowego Funduszu;
9) przedkładanie Sejmowi Rzeczypospolitej Polskiej do dnia 31 sierpnia następnego roku sprawozdania rocznego z działalności Funduszu przygotowanego w trybie, o którym mowa w art. 187;
9a) powoływanie i odwoływanie Prezesa Funduszu, zastępców Prezesa Funduszu, członków Rady Funduszu i dyrektorów oddziałów wojewódzkich Funduszu;
10) sprawowanie nadzoru nad Agencją;
11) zatwierdzanie sprawozdań finansowych Agencji;
12) opracowywanie, ustalanie i aktualizowanie mapy potrzeb zdrowotnych, o której mowa w art. 95a ust. 1;
13) opracowywanie, ustalanie, monitorowanie i aktualizowanie krajowego planu transformacji, o którym mowa w art. 95b ust. 1;
14) ocena projektu wojewódzkiego planu transformacji, o którym mowa w art. 95c ust. 1, i jego zatwierdzanie;
15) wydawanie opinii o celowości inwestycji, o której mowa w art. 95d ust. 1.

Powyższe przepisy w sposób jednoznaczny przesądzają, że administratorem danych osobowych lekarza, które zostały pozyskane z systemu [...] wbrew wynikającym z tych przepisów celach (o czym bardziej szczegółowo będzie mowa w dalszej części niniejszej decyzji), a następnie opublikowane na platformie społecznościowej X (dawniej Twitter) jest Minister Zdrowia, a nie osoba fizyczna powołana

na to stanowisko. To bowiem Minister Zdrowia, w świetle ww. przepisów, został wyposażony w określone uprawnienia pozwalające mu na dostęp w ściśle zdefiniowanych przypadkach i w określonych celach do danych przetwarzanych w systemie [...]. Naruszenie tych zasad przy dostępie do danych osobowych nie może jednak powodować utraty przez Ministra Zdrowia statusu administratora i uznania za takiego administratora innego podmiotu (lub osoby). Wręcz przeciwnie, działanie wbrew zasadom przetwarzania danych osobowych opisanym w ww. przepisach prawa, nie tylko bowiem potwierdza naruszenie tych przepisów oraz przepisów rozporządzenia 2016/679 dotyczących podstaw prawnych przetwarzania danych, ale również świadczy o niewdrożeniu odpowiednich środków bezpieczeństwa mających zapewnić ochronę danych w systemie [...], w tym przed dostępem do nich w sposób niezgodny z przepisami ustawy o systemie informacji w ochronie zdrowia oraz wykorzystaniem w celach innych niż określone w ww. ustawie. Podkreślić bowiem należy, że Minister Zdrowia odpowiada zarówno za pozyskiwanie danych z zarządzanych przez siebie zasobów informacyjnych zgodne z przepisami szczególnymi i tylko w celach wskazanych w tych przepisach, jak i bierze odpowiedzialność za ich dalsze przetwarzanie, tj. - w tym przypadku – opublikowanie tych danych na platformie społecznościowej X (dawniej Twitter). Z tego względu zakresem niniejszego postępowania administracyjnego objęto również naruszenie tych przepisów rozporządzenia 2016/679, które odnoszą się do kwestii bezpieczeństwa danych, i za przestrzeganie których odpowiedzialność ponosi administrator, a więc Minister Zdrowia. Nie ulega bowiem wątpliwości, że opracowanie i prawidłowe wdrożenie w szczególności środków bezpieczeństwa o charakterze organizacyjnym, np. w postaci odpowiednich procedur, mogłoby zapobiec naruszeniu ochrony danych osobowych, które zostało zgłoszone Prezesowi UODO w dniu 9 sierpnia 2023 r. Podkreślić również należy, że ww. zgłoszenie naruszenia ochrony danych osobowych, dokonane przez Ministra Zdrowia, nie dotyczyło wyłącznie faktu ujawnienia danych osobowych lekarza na platformie społecznościowej X (dawniej Twitter), ale także naruszenia zasad bezpieczeństwa związanego z pozyskaniem tych danych z systemu [...] oraz sposobu ich przekazania Ministrowi Zdrowia (za pomocą komunikatora Whatsapp). W tym kontekście, dla uznania organu administracji publicznej, tj. Ministra Zdrowia, za administratora tych danych i adresata niniejszej decyzji, bez znaczenia pozostaje miejsce, w którym doszło do opublikowania danych osobowych lekarza, gdyż Minister Zdrowia nie miał podstaw do publikacji danych osobowych lekarza na jakimkolwiek profilu społecznościowym. Ponadto należy zaznaczyć, iż rozstrzygnięcia zawarte w niniejszej decyzji nie wyczerpują wszystkich aspektów sprawy, a w szczególności nie przesądzają o braku osobistej odpowiedzialności osoby sprawującej funkcję Ministra Zdrowia za działania, których skutkiem było naruszenie ochrony danych osobowych lekarza, jego praw i wolności chronionych przepisami rozporządzenia 2016/679 oraz jego dóbr osobistych. Poza innymi uprawnieniami lekarza leżącymi poza zakresem kompetencji Prezesa UODO (np. możliwością wystąpienia z roszczeniami cywilnoprawnymi), przysługuje mu bowiem jeszcze prawo złożenia do Prezesa UODO skargi na niezgodne z prawem przetwarzanie jego danych osobowych przez Ministra Zdrowia działającego „prywatnie” jako osoba fizyczna.

Art. 5 rozporządzenia 2016/679 określa zasady dotyczące przetwarzania danych osobowych, które muszą być respektowane przez wszystkich administratorów, tj. podmioty, które samodzielnie lub wspólnie z innymi ustalają cele i sposoby przetwarzania danych osobowych. W myśl art. 5 ust. 1 lit. a) rozporządzenia 2016/679, dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"). Stosownie zaś do art. 5 ust. 2 rozporządzenia 2016/679, administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Zgodnie z art. 6 ust. 1 rozporządzenia 2016/679 przetwarzanie danych osobowych jest zgodne z prawem wyłącznie gdy spełniony jest co najmniej jeden z poniższych warunków:
a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Należy zaznaczyć, że przepis art. 6 ust. 1 lit. f) rozporządzenia 2016/679 nie ma zastosowania do przetwarzania danych osobowych przez organy publiczne w ramach realizacji swoich zadań.

Art. 9 ust.1 rozporządzenia 2016/679 zabrania przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Motyw 35 rozporządzenia 2016/679 uszczegóławia pojęcie danych osobowych dotyczących zdrowia wskazując, że „Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą".

Wskazać również należy, że w myśl art. 4 pkt 2) rozporządzenia 2016/679, „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Dla oceny dopuszczalności wykorzystywania przez Ministra Zdrowia danych osobowych przetwarzanych w systemie [...] niezbędne jest odniesienie się do stanowisk wypracowanych w orzecznictwie Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości Unii Europejskiej, dotyczących rejestrów publicznych, gdyż, jak należy przyjąć z uwagi na treść art. 5 ust. 2 i art. 7 ust. 1 ustawy o systemie informacji w ochronie zdrowia, taki charakter ma ww. system, w tym do orzeczeń wypracowanych w wyniku analizy przepisów o rejestrach medycznych, jako elementu systemu informacji, o którym mowa w art. 5 ust. 1 tej ustawy, obsługiwanego przez system [...]. Należy zatem wskazać, iż samo tworzenie rejestrów medycznych, jak podkreśla Trybunał Konstytucyjny w wyroku z dnia 18.12.2014 r., K 33/13, OTK-A 2014, nr 11, poz. 120 *„(...) może być uznane za niezbędne w demokratycznym państwie prawnym (art. 51 ust. 2 Konstytucji). Zarówno monitorowanie zapotrzebowania na świadczenia opieki zdrowotnej oraz stanu zdrowia obywateli, jak i prowadzenie profilaktyki zdrowotnej i realizacja programów zdrowotnych służą zapewnieniu bezpieczeństwa publicznego oraz zdrowia (art. 31 ust. 3 Konstytucji). Uwzględnienie tych wartości może przemawiać za ograniczeniem konstytucyjnych wolności i praw, jeśli zakres i formy tego ograniczenia spełniają przesłankę konieczności oraz nie naruszają istoty wolności i praw".* Podobne stanowisko w sprawach dotyczących publicznych rejestrów prezentuje Trybunał Sprawiedliwości Unii Europejskiej (TSUE), wielokrotnie podkreślając, iż *„udostępnianie danych osobowych podmiotowi trzeciemu, takiemu jak organ władzy publicznej, stanowi ingerencję w zagwarantowane w art. 7* ***[1]*** *i 8* ***[2]*** *karty prawa podstawowe niezależnie od tego, w jaki sposób te dane zostaną później wykorzystane"* [podobnie wyroki: z dnia 20 maja 2003 r., Österreichischer Rundfunk i in., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, pkt 74 i 75; a także z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 33–36; a także opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 124, 126]. Zgodnie z orzecznictwem TSUE, prawa zagwarantowane w art. 7 i 8 karty praw podstawowych Unii Europejskiej nie mogą zostać uznane za stanowiące prerogatywy o charakterze absolutnym, lecz powinny być oceniane w świetle ich funkcji społecznej. W związku z tym dane osobowe powinny być przetwarzane w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Ponadto, zgodnie z wyrokiem TSUE z dnia 16 lipca 2020 r. w sprawie C-311/18, ECLI:EU:C:2020:559 *„(...) aby spełnić wymóg proporcjonalności, zgodnie z którym odstępstwa od ochrony danych osobowych i jej ograniczeń mogą być stosowane jedynie wtedy, gdy jest to absolutnie konieczne – powinno zawierać jasne i precyzyjne reguły dotyczące zakresu i stosowania rozpatrywanego środka oraz ustanawiać minimalne wymagania służące temu, aby osoby, których dane osobowe zostały przekazane, były zaopatrzone w wystarczające zabezpieczenia umożliwiające rzeczywistą ochronę ich danych przed*

ryzykiem nadużyć. Powinno ono w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać przyjęty środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja będzie ograniczona do tego, co ściśle konieczne".

Art. 47 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.) podkreśla, iż każda osoba ma prawo doochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Trybunał Konstytucyjny w swoich wyrokach odnosił się właśnie do tego przepisu wskazując, że prawo do prywatności obejmuje także informacje o stanie zdrowia, co zostało podkreślone w orzeczeniu z 24 czerwca 1997 r., sygn. K 21/96, OTK ZU nr 2/1997, poz. 23 oraz wyroku z 20 listopada 2002 r., sygn. K 41/02, OTK ZU nr 6/A/2002, poz. 83.

Z orzecznictwa TSUE oraz TK wynika zatem jednoznacznie, że udostępnianie osobom trzecim danych osobowych znajdujących się w publicznych rejestrach stanowi naruszenie podstawowych praw i wolności osób fizycznych, godzi w ich prywatność oraz pociągnąć może za sobą poważne konsekwencje materialne oraz niematerialne.

Naruszenie przez Ministra Zdrowia ochrony danych osobowych lekarza skutkujące wydaniem niniejszej decyzji dotyczy danych osobowych przetwarzanych w systemie [...]. Nie ulega wątpliwości, że dane osobowe znajdujące się w tym systemie należą do szczególnych kategorii danych osobowych i jako takie podlegają szczególnej ochronie. Istotny jest również fakt, iż podmioty, które posiadają dostęp do tego systemu, zostały ściśle określone przepisami ustawy o systemie informacji w ochronie zdrowia (w art. 7 ust. 1) wraz z precyzyjnym wskazaniem celów, dla których taki dostęp mogą realizować, co stanowi o wadze przetwarzanych w nich danych i ma stanowić dodatkowe gwarancje dla tych danych. Przepisy te wykluczają zatem nie tylko bezpośredni dostęp osób nieuprawnionych do danych osobowych znajdujących się w systemie [...], ale również ograniczają możliwość ich wykorzystania przez podmioty uprawnione w celach innych niż określone przepisami prawa.

W omawianym przypadku Minister Zdrowia dopuścił się pozyskania danych osobowych lekarza z systemu [...] w celach niewynikających z ustawy o systemie informacji w ochronie zdrowia, a następnie ich publikacji na portalu społecznościowym X (dawniej Twitter). Podkreślić należy, że recepty *„pro auctore"* lekarz może wystawić na własne potrzeby, zatem, jak sama nazwa wskazuje, leki przepisywane przez lekarza za pomocą tej kategorii recept przeznaczone są do jego wyłącznego użytku. Dane dotyczące przepisanych za pomocą takiej recepty leków, jako że jednoznacznie mogą wskazywać na schorzenia, stanowią dane dotyczące zdrowia wystawiającego je lekarza, a zatem dane podlegające szczególnej ochronie na gruncie art. 9 ust. 1 rozporządzenia 2016/679. Ujawnienie danych dotyczących zdrowia, bez wątpienia godzi w prawo do prywatności lekarza, którego dane dotyczą. Jak sam Administrator wskazuje w zgłoszeniu naruszenia ochrony danych osobowych, *„Z uwagi na kontekst medialny i polityczny naruszenia ochrony danych osobowych polegający na*

upublicznieniu danych osobowych osoby fizycznej reprezentującej środowisko lekarskie oraz z uwagi na informację o wystawionym przez lekarza leku naruszenie może prowadzić co najmniej do domniemania o stanie zdrowia czyli danej szczególnej kategorii. Ujawnienie tej informacji może dla osoby fizycznej (lekarza) mieć konsekwencje osobiste chociażby związane z wykonywaniem pracy ze względu na upublicznienie informacji o miejscu pracy. Ponadto z uwagi na tło polityczne sprawy osoba, której dane dotyczą może spotkać się z nieprzyjemnościami wynikającymi z różnic poglądów od osób, z którymi wchodzi w interakcje, co wydaje się prawdopodobne z uwagi na fakt, że sprawa publikacji danych była szeroko komentowana w różnych mediach". TSUE w wyroku z dnia 22 listopada 2022 r. dotyczącego połączonych spraw C-37/20 i C-601/20, ECLI:EU:C:2022:912, podkreśla iż *„(...) potencjalnie konsekwencje dla zainteresowanych osób wynikające z ewentualnego niewłaściwego wykorzystania ich danych osobowych pogłębia fakt, że po ich publicznym udostępnieniu dane te mogą być nie tylko swobodnie przeglądane, ale także przechowywane i rozpowszechniane, a w przypadku takiego kolejnego przetwarzania trudniejsza, a nawet iluzoryczna staje się dla tych osób skuteczna obrona przed niewłaściwym wykorzystaniem".*

W tym miejscu należy ponownie wskazać, iż Minister Zdrowia dopuścił się przetwarzania danych osobowych lekarza w celu niezgodnym z ustawą o systemie informacji w ochronie zdrowia. Przypomnieć zatem należy, że ww. ustawa w art. 7 ust. 1 pkt 8 stanowi, iż system [...] umożliwia ministrowi właściwemu do spraw zdrowia dostęp do danych niezbędnych do realizacji zadań określonych w art. 11 ust. 1 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2022 r. poz. 2561). Przepis ten enumeratywnie wymienia przypadki, w których dopuszczalne jest przetwarzanie danych osobowych znajdujących się w systemie [...] przez Ministra Zdrowia, a należy do nich m.in. prowadzenie oraz współuczestniczenie w prowadzeniu edukacji w zakresie zapobiegania i rozwiązywania problemów związanych z negatywnym wpływem na zdrowie czynników środowiskowych i społecznych; prowadzenie działań związanych z promocją zdrowia i profilaktyką chorób; opracowywanie, finansowanie i ocena efektów programów polityki zdrowotnej, a także nadzór nad ich realizacją; kwalifikowanie świadczeń opieki zdrowotnej jako świadczeń gwarantowanych; planowanie, przekazywanie i rozliczanie dotacji z budżetu państwa; współdziałanie z organizacjami pozarządowymi o charakterze regionalnym lub ogólnokrajowym działającym na rzecz ochrony zdrowia oraz sprawowanie nadzoru nad ubezpieczeniem zdrowotnym; przedkładanie Sejmowi Rzeczypospolitej Polskiej sprawozdania rocznego z działalności Funduszu. Art. 11 ust. 1 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznychnie przewiduje pozyskiwania danych osobowych z systemu [...] przez Ministra Zdrowia w celu ich publikacji np. na platformach społecznościowych dla *„obrony dobrego imienia Ministerstwa Zdrowia"* oraz *„obrony interesów pacjenta"*. Takie działanie Ministra Zdrowia jest także w konsekwencji niezgodne z Konstytucją RP, która w art. 7 wskazuje, że organy władzy publicznej działają na podstawie i w granicach prawa.

Powyższe przesądza zatem jednoznacznie, że pozyskanie z systemu [...] przez Ministra Zdrowia danych osobowych lekarza w zakresie imienia, nazwiska oraz danych dotyczących zdrowia (informacji

o wystawionej recepcie „pro auctore" na leki z grupy psychotropowych i przeciwbólowych), jako niezgodne z celami przetwarzania danych osobowych określonymi w ww. przepisach prawa, nastąpiło bez podstawy prawnej, a w konsekwencji z naruszeniem art. 6 ust. 1 oraz art. 9 ust. 1 rozporządzenia 2016/679, co jednocześnie stanowi o naruszeniu zasady zgodności z prawem wyrażonej w art. 5 ust. 1 lit. a) rozporządzenia 2016/679. Tym samym, Minister Zdrowia, ujawniając publicznie dane osobowe lekarza w ww. zakresie, odebrał mu jego konstytucyjne prawo do ochrony prawnej życia prywatnego i decydowania o jego życiu osobistym. Wskazać także należy, że sam Administrator dostrzegł nieprawidłowości w swoim działaniu przyznając w piśmie z dnia 27 września 2023 r., że *„Publikacja danych osobowych pochodzących z systemu [...] nie miała podstaw w przepisach prawa powszechnie obowiązującego*".

Podkreślić należy, że karygodna jest sytuacja, w której Minister Zdrowia wykorzystuje dane osobowe znajdujące się w specjalistycznych rejestrach do celów innych niż określone w przepisach prawa. Minister Zdrowia wykorzystując swoje uprawnienia wynikające z pełnionej funkcji, wydając swoim pracownikom polecenie pozyskania z systemu [...] i przekazania mu danych osobowych lekarza nadużył stanowiska, a publikując te dane na portalu społecznościowym X (dawniej Twitter) nadużył zaufania obywateli, którzy na skutek zaistniałego naruszenia nie mogą mieć pewności, czy również ich dane są należycie chronione.

Tym samym Prezes UODO stwierdził naruszenie przez Ministra Zdrowia art. 5 ust. 1 lit. a) rozporządzenia 2016/679 w związku z przetwarzaniem danych osobowych ww. osoby bez podstawy prawnej, a więc z naruszeniem art. 6 ust. 1 i art. 9 ust. 1 rozporządzenia 2016/679, a w konsekwencji art. 5 ust. 2 rozporządzenia 2016/679, tj. zasady rozliczalności.

Zgodnie z art. 5 ust. 1 lit. f) rozporządzenia 2016/679, dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („poufność i integralność"). Stosownie zaś do art. 5 ust. 2 rozporządzenia 2016/679, administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność"). Konkretyzację zasady poufności, o której mowa w art. 5 ust. 1 lit. f) rozporządzenia 2016/679, stanowią dalsze przepisy tego aktu prawnego. Zgodnie z art. 24 ust 1 rozporządzenia 2016/679, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

W myśl z art. 25 ust. 1 rozporządzenia 2016/679, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub

wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

Z treści art. 32 ust. 1 rozporządzenia 2016/679 wynika, że administrator jest zobowiązany do zastosowania środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Przepis precyzuje, że decydując o środkach technicznych i organizacyjnych należy wziąć pod uwagę stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Z przytoczonego przepisu wynika, że ustalenie odpowiednich środków technicznych i organizacyjnych jest procesem dwuetapowym. W pierwszej kolejności istotnym jest określenie poziomu ryzyka, jakie wiąże się z przetwarzaniem danych osobowych uwzględniając przy tym kryteria wskazane w art. 32 ust. 1 rozporządzenia 2016/679, a następnie należy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Ustalenia te, w stosownym przypadku, powinny obejmować środki takie, jak pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W myśl art. 32 ust. 2 rozporządzenia 2016/679, administrator oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Przytoczone w części II niniejszej decyzji przepisy prawa oraz przywołane orzeczenia TSUE i TK wskazują na wagę zaistniałego naruszenia ochrony danych osobowych, którego dopuścił się Minister Zdrowia. Wynikająca z nich w sposób jednoznaczny wrażliwość danych osobowych przetwarzanych w rejestrach publicznych, w tym w systemie [...], determinuje obowiązek dla administratora danych wprowadzenia odpowiednich środków bezpieczeństwa, które nie tylko zapewnią ochronę dla tych danych osobowych, ale będą budować poczucie wśród społeczeństwa, że ich dane będą wykorzystywane wyłącznie w uzasadnionych i określonych przepisami prawa celach. W tym kontekście szczególnego znaczenia nabierają przede wszystkim środki bezpieczeństwa o charakterze organizacyjnym, gdyż to one mogą przeciwdziałać w pierwszej kolejności wszelkim

nadużyciom i wykorzystywaniu danych zgromadzonych w rejestrach publicznych, w tym w systemie [...], w celach niezgodnym ze wskazanymi w odpowiednich przepisach.

Dobór odpowiednich środków bezpieczeństwa, a więc zarówno tych o charakterze technicznym i organizacyjnym, powinien zostać poprzedzony analizą ryzyka, na podstawie której Administrator identyfikuje zagrożenia dla przetwarzanych danych osobowych oraz ustala stopień ryzyka naruszenia praw lub wolności osób fizycznych w sytuacji np. wystąpienia naruszenia poufności tych danych.

W tym miejscu wskazać należy, iż rozporządzenie 2016/679 wprowadziło podejście, w którym zarządzanie ryzykiem stanowi fundament działań związanych z ochroną danych osobowych. Zarządzanie ryzykiem ma charakter ciągłego procesu wymuszającego na administratorze nie tylko zapewnienie zgodności z przepisami rozporządzenia 2016/679 poprzez jednorazowe wdrożenie organizacyjnych i technicznych środków bezpieczeństwa, ale także zapewnienie ciągłości monitorowania poziomu zagrożeń oraz zapewnienie rozliczalności w zakresie poziomu oraz adekwatności wprowadzonych zabezpieczeń. Wobec powyższego, koniecznością staje się możliwość udowodnienia przed organem nadzorczym, że wprowadzone rozwiązania, mające na celu zapewnienie bezpieczeństwa danych osobowych, są adekwatne do poziomu ryzyka, jak również uwzględniają charakter danej organizacji oraz wykorzystywanych mechanizmów przetwarzania danych osobowych. Administrator samodzielnie ma zatem przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka. Konsekwencją takiego podejścia jest konieczność samodzielnego doboru zabezpieczeń w oparciu o analizę zagrożeń. Administratorom nie są wskazywane konkretne środki i procedury w zakresie bezpieczeństwa. W wyroku z 26 sierpnia 2020 r., sygn. II SA/Wa 2826/19, Wojewódzki Sąd Administracyjny w Warszawie wskazał, że *„Przepis ten* [art. 32 rozporządzenia 2016/679] *nie wymaga od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różną wysokością.”*, *„Przyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka.”*, a także *„(...) czynności o charakterze techniczno – organizacyjnym leżą w gestii administratora danych osobowych, ale nie mogą być dobierane w sposób całkowicie swobodny i dobrowolny, bez uwzględnienia stopnia ryzyka oraz charakteru chronionych danych osobowych.”*

Wobec powyższego, to odpowiednio przeprowadzona analiza ryzyka zapewnia administratorowi możliwość określenia i wprowadzenia środków technicznych i organizacyjnych, które spowodują wyeliminowanie lub co najmniej znaczne obniżenie ustalonego poziomu ryzyka materializacji

zidentyfikowanych zagrożeń dla przetwarzanych danych osobowych. Ocena ryzyka przeprowadzona przez administratora powinna zostać udokumentowana oraz uzasadniona stanem faktycznym istniejącym w chwili jej przeprowadzania. Główne czynniki składające się na prawidłową ocenę, które powinny zostać wzięte pod uwagę podczas przeprowadzania analizy, to charakterystyka zachodzących procesów przetwarzania, aktywa, podatności, zagrożenia oraz aktualne zabezpieczenia. Należy pamiętać, iż istotne przy ocenianiu ryzyka są również takie czynniki, jak zakres i charakter przetwarzanych przez administratora danych osobowych, gdyż to od nich zależeć będą ewentualne negatywne skutki dla osoby fizycznej występujące w momencie naruszenia ochrony jej danych osobowych.

Administrator wraz z pismem z dnia 16 sierpnia 2023 r. przedstawił arkusz analizy ryzyka w związku z nieuprawnionym uzyskaniem dostępu do danych przetwarzanych przy wykorzystaniu systemu [...]. Brak jest informacji wskazującej na datę przeprowadzenia tej analizy, przedstawiony arkusz ryzyk opisany jest jako „ryzyka aktualne". W przedstawionym arkuszu Administrator przewidział określone ryzyka dla danych, takie jak np. „Ryzyko - dostęp do bazy danych dla nieuprawnionych użytkowników", „Ryzyko przetwarzania danych osobowych bez podstawy prawnej" oraz „Ryzyko utraty bezpieczeństwa informacji spowodowane przypadkowym lub celowym działaniem pracownika w systemie [...]". Analiza opisu ryzyka oraz jego przyczyny pozwala na przyjęcie, że najbardziej zbliżone do sytuacji będącej przedmiotem niniejszego postępowania administracyjnego jest „Ryzyko utraty bezpieczeństwa informacji spowodowane przypadkowym lub celowym działaniem pracownika w systemie [...]", gdyż jako przyczynę wskazano niską świadomość pracowników w zakresie wrażliwości danych przetwarzanych w systemie oraz stosowanie procedur bezpieczeństwa w niewystarczającym zakresie (gdy tymczasem w przypadku „Ryzyka przetwarzania danych osobowych bez podstawy prawnej" taką przyczyną są „Zmiany legislacyjne w zakresie przetwarzania danych osobowych, brak komunikacji pomiędzy komórkami organizacyjnymi przetwarzającymi dane osobowe a IOD"). „Ryzyko utraty bezpieczeństwa informacji spowodowane przypadkowym lub celowym działaniem pracownika w systemie [...]" określone zostało na poziomie średnim, a środki bezpieczeństwa proponowane przez Administratora to wprowadzenie cyklicznych szkoleń uświadamiających z zakresu bezpieczeństwa i cyberbezpieczeństwa danych.

Nawet gdyby przyjąć, że tak opisane ryzyko obejmuje sytuację przekazania danych osobowych z systemu [...] podmiotowi uprawnionemu, ale wbrew celom określonym w przepisach prawa, a następnie ich opublikowanie np. na platformie społecznościowej, to i tak zaproponowane środki w celu wyeliminowania lub co najmniej ograniczenia tego ryzyka nie są odpowiednie, gdyż same szkolenia z zakresu bezpieczeństwa i cyberbezpieczeństwa danych nie pozwolą na osiągnięcie tego celu, bez wprowadzenia właściwych procedur, które określą sposób postępowania w takiej sytuacji. Dostrzegł to również Administrator, który po naruszeniu ochrony danych osobowych przystąpił do opracowywania procedury pn. „ [...]". Ponadto, rekomendacje w tym zakresie zostały sformułowane w „Sprawozdaniu [...]" (nr zadania [...]) z dnia (...) października 2023 r., gdzie wskazano m.in., że „Wymagana jest zmiana Porozumienia przez C. wraz z Ministerstwem Zdrowia w części dotyczącej

wydawania poleceń przez Ministra Zdrowia w taki sposób, aby ewentualne polecenia wydawane były w trybie oficjalnym i zawierały sformułowanie „polecenie" (zamiast za pomocą poczty elektronicznej) oraz wprowadzenie zakazu stosowania innych kanałów komunikacji nieokreślonych w Porozumieniu [a więc np. komunikatora Whatsapp – uwaga własna]", „Wprowadzenie procesu lub zarządzenia w zakresie uzyskiwania przez pracowników (w tym członków kierownictwa) Ministerstwa Zdrowia danych osobowych gromadzonych w systemach teleinformatycznych obsługiwanych przez C. (systemy, o których mowa w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia ze szczególnym uwzględnieniem uprzedniego stanowiska Pełnomocnika ds. Bezpieczeństwa Informacji oraz Inspektora Ochrony Danych (jako element konieczny i niezbędny)" oraz „Wprowadzenie w Ministerstwie Zdrowia procesu/zarządzenia obejmującego obszar udostępnień danych osobowych, których administratorem jest Minister Zdrowia na rzecz uprawnionych podmiotów i instytucji obejmujący centralny rejestr wniosków obejmujących ich realizację". Podkreślić należy, że procedur, o których mowa w ww. rekomendacjach, nie zastąpi procedura funkcjonująca w C. „[...]", gdyż podmiot ten jest wyłącznie administratorem systemu, stosownie do art. 7 ust. 2 ustawy o systemie informacji w ochronie zdrowia, a procedury w tym zakresie muszą być opracowane i wdrożone przez administratora, a więc przez Ministra Zdrowia. Biorąc pod uwagę, że naruszenie ochrony danych osobowych spowodowane było działaniami samego Administratora wydaje się, że celowym byłoby jednak, aby tego typu ryzyko opisane było odrębnie, co zapewni dobór ściśle dedykowanym temu ryzyku środków bezpieczeństwa, uwzględniających także specyfikę relacji związanych z podległością służbową.

Ryzyko w tym zakresie dodatkowo zwiększa fakt wykorzystania do przekazania danych osobowych lekarza pozyskanych z systemu [...] Ministrowi Zdrowia za pomocą komunikatora WhatsApp, którego to kanału przekazywania danych nie zidentyfikowano w przeprowadzonej analizie ryzyka. Wykorzystany przez Ministra Zdrowia środek przekazu nie może zostać uznany za taki, który może być stosowany do komunikowania się przez organy administracji publicznej z uwagi na wykazane naruszenia przepisów rozporządzenia 2016/679. Właściciel komunikatora WhatsApp w 2021 r. został ukarany przez irlandzki organ nadzorczy (Data Protection Comission, dalej DPC) administracyjną karą pieniężną w wysokości 225 mln euro za brak przejrzystości w przetwarzaniu danych osobowych, przejawiającą się między innymi brakiem wskazania, jakie dane osobowe i w jakich sytuacjach udostępniane są innym aplikacjom i innym podmiotom należącym do grupy kapitałowej Facebook (Meta). Stosunkowo niedawno, bo 12 stycznia 2023 r. WhatsApp Ireland Limited ponownie został ukarany przez DPC administracyjną karą pieniężną w wysokości 5,5 mln euro wraz z nakazem dostosowania operacji przetwarzania do przepisów rozporządzenia 2016/679[3], w następstwie wiążącej decyzji Europejskiej Rady Ochrony Danych (EROD) z dnia 5 grudnia 2022 r. wydanej na podstawie art. 63 oraz art. 65 rozporządzenia 2026/679 w ramach mechanizmu spójności, w związku z niedopełnieniem obowiązku w zakresie transparentności. W decyzji DPC wskazał, że informacje dotyczące podstawy prawnej, na której oparł przetwarzanie WhatsApp IE, nie zostały jasno przedstawione użytkownikom, co spowodowało, że użytkownicy nie mieli wiedzy na temat tego, jakie operacje przetwarzania są prowadzone na ich danych osobowych oraz w jakim celu. EROD wydała

postanowienie, na podstawie którego ustalono, iż utrzymane zostało stanowisko DPC jako organu wiodącego dotyczące naruszenia wymogów przejrzystości, tj. art. 5 ust. 1 lit a) rozporządzenia 2016/679.

Wykorzystanie wskazanego komunikatora przy jednoczesnym braku wprowadzonej procedury regulującej zasady wnioskowania o przekazanie danych osobowych zgromadzonych w systemach teleinformatycznych, a zatem i w systemie [...], oznacza brak zastosowania jakichkolwiek środków bezpieczeństwa przy przetwarzaniu danych osobowych lekarza, którego dane osobowe finalnie zostały ujawnione przez Ministra Zdrowia na platformie społecznościowej X (dawniej Twitter). Co więcej, wykazane w ww. decyzjach DPC naruszenia przepisów rozporządzenia 2016/679 przez właściciela tego komunikatora w istocie zwiększają tylko ryzyka niezgodnego z prawem wykorzystania tych danych, choćby z uwagi na potencjalny dostęp do tych danych przez inne podmioty wchodzące w skład grupy kapitałowej Meta. Brak analizy ryzyka w tym zakresie uniemożliwił Ministrowi Zdrowia także identyfikację innych zagrożeń związanych np. z bezpieczeństwem, które mogą powodować naruszenie praw lub wolności osób, których dane są przetwarzane w systemie [...], oraz mogą prowadzić do poważnych konsekwencji takiego naruszenia związanych z całkowitą utratą kontroli przekazanych za pośrednictwem ww. komunikatora danych osobowych.

Podkreślenia wymaga także fakt, że w raporcie z audytu przeprowadzonego w C. zakończonego w dniu 30 października 2023 r. wskazano, w punkcie 2 tego raportu, iż Polityka bezpieczeństwa danych osobowych obowiązująca w instytucji odwołuje się do nieaktualnych przepisów, jak również, że stosowane jest stare podejście do ochrony danych osobowych. Jednym z zaleceń sformułowanych po audycie jest „Opracować politykę bezpieczeństwa danych zgodną z RODO". Raport wskazuje na konieczność dostosowania stopnia bezpieczeństwa operacji przetwarzania do stopnia ryzyka związanego z każdą z operacji. Wskazuje to na niską świadomość pracowników odpowiedzialnych za przetwarzanie danych osobowych w C., co w jeszcze większym stopniu powinno przyczynić się do podjęcia działań przez Ministerstwo Zdrowia w celu poprawy jakości bezpieczeństwa danych osobowych, których administratorem jest Minister Zdrowia, a które przetwarzane są przez C. jako administratora systemu.

Finalnie stwierdzić należy, że przekazując dane osobowe lekarza za pomocą komunikatora WhatsApp Administrator stworzył możliwość utraty przez niego kontroli nad tymi danymi, w tym ich bezpieczeństwem.

Podkreślenia wymaga fakt, że stosując przepisy rozporządzenia 2016/679 należy brać pod uwagę to, iż celem niniejszej regulacji jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych, co zostało zawarte w art. 1 ust. 2 tego aktu prawnego. W przypadku pojawienia się jakichkolwiek wątpliwości w związku z koniecznością

wykonania obowiązków wynikających z rozporządzenia 2016/679 administrator zobowiązany jest w pierwszej kolejności brać pod uwagę właśnie te wartości.

Wobec braku zastosowania przez Administratora adekwatnych środków bezpieczeństwa mających na celu zapewnić ochronę danych przetwarzanych za pomocą systemu [...], należy stwierdzić, że Minister Zdrowia nie zapewnił odpowiedniego poziomu zabezpieczenia danych przetwarzanych przy jego użyciu. Przesądza to o naruszeniu przez Administratora obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych w czasie przetwarzania danych osobowych, aby przetwarzanie to odbywało się zgodnie z rozporządzeniem 2016/679 i w celu nadania przetwarzaniu niezbędnych zabezpieczeń, do czego był on zobowiązany zgodnie z art. 24 ust 1 i 25 ust. 1 rozporządzenia 2016/679, jak również obowiązku zastosowania środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych poprzez m.in. zdolność do ciągłego zapewnienia poufności tych danych, do czego zobowiązuje administratora art. 32 ust. 1 rozporządzenia 2016/679, przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem danych osobowych, o którym mowa w art. 32 ust. 2 rozporządzenia 2016/679, a w konsekwencji również o naruszeniu zasady poufności wyrażonej w art. 5 ust 1 lit. f) rozporządzenia 2016/679, której ww. przepisy są uszczegółowieniem. Efektem zaś naruszenia zasady poufności jest naruszenie art. 5 ust. 2 rozporządzenia 2016/679. Jak bowiem wskazał Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 10 lutego 2021 r. (sygn. II SA/Wa 2378/20, Legalis nr 2579568), „(...) administrator danych jest odpowiedzialny za przestrzeganie wszystkich zasad przy przetwarzaniu danych osobowych (wymienionych w art. 5 ust. 1) i musi być w stanie wykazać ich przestrzeganie. Zasada rozliczalności bazuje więc na prawnej odpowiedzialności administratora za właściwe wypełnianie obowiązków i nakłada na niego obowiązek wykazania zarówno przed organem nadzorczym, jak i przed podmiotem danych, dowodów na przestrzeganie wszystkich zasad przetwarzania danych". Podobnie kwestię tę zinterpretował Wojewódzki Sądu Administracyjny w Warszawie z dnia 26 sierpnia 2020 r. (sygn. II SA/Wa 2826/19, Legalis nr 2480051), stwierdzając, iż „[b]iorąc pod uwagę całość norm rozporządzenia 2016/679, podkreślić należy, że administrator ma znaczną swobodę w zakresie stosowanych zabezpieczeń, jednocześnie jednak ponosi odpowiedzialność za naruszenie przepisów o ochronie danych osobowych. Z zasady rozliczalności wprost wynika, że to administrator powinien wykazać, a zatem udowodnić, że przestrzega zasadę określoną w art. 5 ust. 1 rozporządzenia 2016/679".

W myśl 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. Zgodnie z art. 34 ust. 2 rozporządzenia 2016/679, zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d). Z kolei stosownie do art. 33 ust. 3 rozporządzenia 2016/679, 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.

W uzupełniającym zgłoszeniu naruszenia ochrony danych osobowych Administrator poinformował, że zawiadomił osobę, której dane dotyczą, o fakcie naruszenia jej danych osobowych oraz przekazał treść tego zawiadomienia. W wyniku przeprowadzonej analizy treści zawiadomienia przekazanego osobie, której dane dotyczą, oraz charakteru zaistniałego naruszenia, czasu trwania, kategorii danych i kategorii osób, których dotyczyło naruszenie oraz zastosowanych środków naprawczych Prezes UODO uznał, że naruszenie poufności danych, w szczególności imienia i nazwiska wraz z danymi dotyczącymi zdrowia, powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w związku z czym konieczne jest ponowne, prawidłowe zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony jej danych osobowych. W przedstawionym przez Administratora zawiadomieniu brakowało bowiem wszystkich informacji wymaganych stosownie do art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679, tj. opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego negatywnych skutków. W związku z powyższym, w dniu 13 września 2023 r. Prezes UODO wystąpił do Administratora o podjęcie działań mających na celu niezwłoczne, ponowne i prawidłowe zawiadomienie osoby, której dane dotyczą oraz wyeliminowanie podobnych nieprawidłowości w przyszłości, poprzez przekazanie tej osobie, w ramach ponownego zawiadomienia o naruszeniu ochrony danych osobowych, opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego negatywnych skutków. W odpowiedzi, pismem z dnia 13 października 2023 r., Administrator przekazał treść powtórnego zawiadomienia skierowanego do osoby, której dane dotyczą.

Analiza treści ponownego zawiadomienia przekazanego lekarzowi wykazała, iż Administrator nie dostosował treści tego pisma do wskazówek przedstawionych w wystąpieniu Prezesa UODO z dnia 13 września 2023 r., gdyż nie ujął w nim prawidłowego, odpowiadającego zakresowi danych osobowych objętych naruszeniem ochrony danych, opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego negatywnych skutków.

Nieprawidłowość przedstawionych podmiotowi danych możliwych konsekwencji naruszenia ochrony danych osobowych przejawia się przede wszystkim w nieprecyzyjnym ich określeniu.
W przedstawionej zanonimizowanej treści ponownego zawiadomienia o naruszeniu ochrony danych osobowych, skierowanego do lekarza, którego dane dotyczą, Administrator wskazał, że *„W wyniku ww. działania mogło dojść do naruszenia poufności danych osobowych. Upublicznienie Pana danych osobowych może prowadzić do domniemania informacji o stanie zdrowia. Istnieje także potencjalne ryzyko, że dane mogą zostać wykorzystane do np. podszycia się w celu wyłudzenia dodatkowych informacji"*. Powyższy opis możliwych konsekwencji jest niewystarczający, aby osoba, której dane dotyczą, mogła zrozumieć, jakie realne konsekwencje naruszenia mogą ją czekać w związku z ujawnieniem jej danych osobowych, w tym danych dotyczących zdrowia. Przede wszystkim, w sytuacji, w której doszło już do ujawnienia danych osobowych, nie można wskazywać podmiotowi danych, że *„mogło dojść do naruszenia poufności danych"*. Takie działanie może wprowadzać osobę, której dane dotyczą, w błąd oraz dawać złudne wrażenie, że w rzeczywistości osoby trzecie nie uzyskały wglądu do danych. Ponadto, opisując możliwe konsekwencje naruszenia ochrony danych osobowych Minister Zdrowia całkowicie pominął fakt ujawnienia na platformie społecznościowej X (dawniej Twitter) danych dotyczących zdrowia, co spowodowało brak przekazania lekarzowi, którego dane dotyczą, informacji o możliwych skutkach naruszenia tej kategorii danych.
W zawiadomieniu Administrator nie zawarł także żadnego opisu środków zaradczych, które samodzielnie może zrealizować osoba, której naruszenie dotyczy, w celu zminimalizowania skutków naruszenia, poprzestając jedynie na opisie działań podjętych przez Ministra Zdrowia.

Jak wskazują Wytyczne 9/2022[4], naruszenie ochrony danych osobowych może potencjalnie wywołać szereg negatywnych skutków dla osób fizycznych, których dane są przedmiotem naruszenia ochrony danych osobowych. Wśród możliwych skutków naruszenia EROD wymienia: uszczerbek fizyczny, szkody materialne lub niemajątkowe. Jako przykłady takich szkód wymienione są m.in.: dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, straty finansowe, naruszenie dobrego imienia, naruszenie poufności danych osobowych oraz znaczna szkoda gospodarcza lub społeczna. Nie ulega wątpliwości, że z uwagi na to, iż naruszeniem ochrony danych osobowych objęte zostały dane dotyczące zdrowia wraz z imieniem i nazwiskiem, to przede wszystkim zaistnieć mogą konsekwencje w postaci dyskryminacji czy naruszenia dobrego imienia osoby, której te dane dotyczą. Nie bez znaczenia dla takiej oceny jest również medialny kontekst naruszenia ochrony danych osobowych oraz rozpoznawalność lekarza związana z jego publicznymi wystąpieniami, co pozwala na jednoznaczną identyfikację tej osoby.

Trzeba mieć także na uwadze, że prawidłowe wykonanie przez Administratora jego obowiązku wynikającego z art. 34 ust. 1 rozporządzenia 2016/679, związane m.in. z koniecznością przekazania w ramach zawiadomienia o naruszeniu ochrony danych osobowych wszystkich wymaganych informacji, stosownie do art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679, nie może być uzależniane od zaistnienia naruszenia praw lub wolności tej osoby w wyniku materializacji możliwych negatywnych konsekwencji naruszenia (por. wyroki Wojewódzkiego Sądu

Administracyjnego w Warszawie z dnia 22 września 2021 r., sygn. II SA/Wa 791/21, z dnia 1 lipca 2022 r., sygn. akt II SA/Wa 4143/21, z dnia 31 sierpnia 2022 r., sygn. akt II SA/Wa 2993/21, z dnia 15 listopada 2022 r., sygn. akt II SA/Wa 546/22 i z dnia 26 kwietnia 2023 r., sygn. akt II SA/Wa 1272/22).

Należy w tym miejscu ponownie podkreślić, iż dane dotyczące zdrowia, zgodnie z rozporządzeniem 2016/679, należą do szczególnych kategorii danych osobowych i jako takie podlegają szczególnym zasadom przetwarzania oraz powinny podlegać szczególnej ochronie ze strony ich administratorów, a w sytuacji wystąpienia naruszenia ochrony danych osobowych powodują powstanie wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej, co obliguje administratora do zawiadomienia takiej osoby o naruszeniu ochrony danych osobowych, w którym muszą znaleźć się informacje określone w art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679. W przypadku przedmiotowego naruszenia ochrony danych osobowych Minister Zdrowia nie przekazał jednak osobie nim objętej wszystkich wymaganych informacji, tj. opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego negatywnych skutków, związanych z naruszeniem danych dotyczących zdrowia. Skutkiem takiego działania Administratora jest możliwość braku pełnego zrozumienia przez podmiot danych wagi zaistniałego naruszenia, natomiast brak wskazania środków proponowanych przez Administratora w celu zaradzenia naruszeniu oraz zminimalizowania jego ewentualnych skutków może nie pozwalać podmiotowi danych podjąć właściwej decyzji odnośnie samodzielnego zabezpieczenia swoich danych przed nieuprawnionym ich wykorzystaniem. EROD w swoich wytycznych wskazuje, iż głównym celem powiadomienia osób fizycznych jest dostarczenie konkretnych informacji o krokach, które powinny one podjąć, aby ochronić się przed negatywnymi konsekwencjami naruszenia ochrony ich danych osobowych. Podkreślenia wymaga, iż proponowane osobie, której dane dotyczą, środki w celu zaradzenia naruszeniu, w tym środki w celu zminimalizowania jego negatywnych skutków, powinny korelować z przedstawionymi tej osobie możliwymi negatywnymi konsekwencjami naruszenia ochrony danych osobowych.

W tym miejscu wskazać należy, iż 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). Prawidłowe wykonanie obowiązku określonego w art. 34 rozporządzenia 2016/679 powinno zapewnić podmiotowi danych szybką i przejrzystą informację o naruszeniu ochrony jego danych osobowych wraz z opisem możliwych konsekwencji naruszenia ochrony danych osobowych oraz środków, które może podjąć w celu zminimalizowania jego ewentualnych negatywnych skutków.

Wobec powyższego należy zaznaczyć, iż aby zachować dbałość o interesy osoby, której dane dotyczą, oraz postępując zgodnie z prawem, Administrator powinien był zapewnić tej osobie

możliwość jak najlepszej, samodzielnej oceny naruszenia jej praw lub wolności w związku z zaistniałym zdarzeniem. Osiągnięcie tego celu wymaga od Administratora skierowania do osoby, której dane dotyczą, co najmniej informacji wymienionych w art. 34 ust. 2 rozporządzenia 2016/679 w formie umożliwiającej podmiotowi danych wielokrotne zapoznanie się z treścią skierowanego do niego zawiadomienia.

W konsekwencji należy stwierdzić, że Administrator zawiadamiając osobę, której dane dotyczą, o naruszeniu jej danych osobowych nie przekazał jej wszystkich wymaganych informacji zgodnie z art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679, tj. opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego negatywnych skutków, co stanowi o naruszeniu tych przepisów przez Ministra Zdrowia.

Oceniając okoliczności przedmiotowego naruszenia ochrony danych osobowych należy podkreślić, że stosując przepisy rozporządzenia 2016/679 należy mieć na uwadze, iż 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 tym miejscu należy zaznaczyć, że 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.

Biorąc pod uwagę powyższe ustalenia oraz stwierdzone naruszenia przepisów rozporządzenia 2016/679, Prezes UODO, korzystając z przysługującego mu uprawnienia określonego w art. 58 ust. 2 lit. i) rozporządzenia 2016/679, zgodnie z którym każdemu organowi nadzorczemu przysługuje uprawnienie do zastosowania, oprócz lub zamiast innych środków naprawczych przewidzianych w art. 58 ust. 2 lit. a)-h) oraz lit. j) tego rozporządzenia, administracyjnej kary pieniężnej na mocy art. 83 ust. 4 lit. a) i ust. 5 lit. a) rozporządzenia 2016/679, mając na względzie okoliczności ustalone

w przedmiotowym postępowaniu stwierdził, iż w rozpatrywanej sprawie zaistniały przesłanki uzasadniające nałożenie na Administratora administracyjnej kary pieniężnej.

Zgodnie z art. 83 ust. 4 lit. a) rozporządzenia 2016/679, naruszenia przepisów dotyczących obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25-39 oraz 42 i 43 podlegają zgodnie z ust. 2 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.

Zgodnie z art. 83 ust. 5 lit. a) rozporządzenia 2016/679, naruszenia przepisów dotyczących podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9, podlegają zgodnie z ust. 2 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.

W niniejszej sprawie administracyjna kara pieniężna wobec Administratora nałożona została za naruszenie art. 25 ust. 1, art. 32 ust. 1 i 2 oraz art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679 na podstawie przytoczonego wyżej art. 83 ust. 4 lit. a) rozporządzenia 2016/679, natomiast za naruszenie art. 5 ust. 1 lit. a) i f), art. 5 ust. 2, art. 6 ust. 1 oraz art. 9 ust. 1 rozporządzenia 2016/679 - na podstawie art. 83 ust. 5 lit. a) tego rozporządzenia.

Decydując o nałożeniu 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, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody (art. 83 ust. 2 lit. a rozporządzenia 2016/679).
Stwierdzone w niniejszej sprawie naruszenie ma znaczną wagę i poważny charakter, stwarza bowiem wysokie ryzyko negatywnych skutków prawnych i faktycznych dla lekarza, którego ujawnione na ww. platformie dane dotyczą. Naruszenie ww. przepisów rozporządzenia 2016/679 pociąga za sobą nie tylko potencjalną, ale również realną możliwość wykorzystania tych danych przez podmioty trzecie bez wiedzy i wbrew woli osoby, której dane dotyczą, niezgodnie z przepisami rozporządzenia 2016/679. Ryzyko wystąpienia szkody w postaci dyskryminacji, utraty dobrego imienia czy utraty zaufania pacjentów niezbędnego w pracy lekarza bez wątpienia zwiększa fakt, iż naruszeniem ochrony danych osobowych objęte zostały dane dotyczące zdrowia w postaci informacji o wystawionej recepcie „pro auctore" na lek z grupy psychotropowych i przeciwbólowych. Ponadto, osoba, której dane ujawniono, może odczuwać obawę przed utratą kontroli nad swoimi danymi

osobowymi, a jak wskazał Sąd Okręgowy w Warszawie w wyroku z dnia 6 sierpnia 2020 r. sygn. akt XXV C 2596/19, obawa, a więc utrata poczucia bezpieczeństwa stanowi realną szkodę niemajątkową wiążącą się z obowiązkiem jej naprawienia. Istotny jest także fakt, że osób objętych ryzykiem naruszenia tożsamego z omawianym w niniejszej decyzji jest więcej, gdyż obejmuje ono wszystkie osoby, których dane są przetwarzane w systemie [...].

W niniejszej sprawie stwierdzono szeroki dostęp do danych osobowych opublikowanych przez Ministra Zdrowia, bowiem post zawierający dane osobowe był szeroko komentowany w mediach. Istotny jest także długi czas trwania naruszenia, bowiem Administrator nie wprowadził odpowiednich środków bezpieczeństwa o charakterze organizacyjnym (np. procedur) mających na celu przeciwdziałanie sytuacji będącej przedmiotem niniejszego postępowania. Ponadto osoba, której dane dotyczą, w dalszym ciągu nie otrzymała pełnej informacji odnośnie naruszenia ochrony jej danych osobowych, zgodnie z art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679.

W niniejszej sprawie naruszenie dotyczyło danych osobowych tylko jednej osoby. Taką liczbę osób dotkniętych naruszeniem, szczególnie wobec faktu, że Minister Zdrowia przy wykorzystaniu systemu [...] przetwarza dane osobowe bardzo dużej liczby osób, należy uznać za niewielką, co niewątpliwie przemawia na korzyść Administratora, lecz nie zmieniło to jednak całościowej oceny, tj. uznania w analizowanej sprawie przesłanki z art. 83 ust. 2 lit. a) rozporządzenia 2016/679 za obciążającą.

2. 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 nr 2016/679 WP253 (przyjętymi w dniu 3 października 2017 r., zatwierdzonymi przez EROD w dniu 25 maja 2018 r.), dalej Wytyczne WP253, umyślność „obejmuje zarówno wiedzę, jak i celowe działanie, w związku z cechami charakterystycznymi czynu zabronionego". Nieuprawniony dostęp do danych osobowych lekarza, którego dane zostały upublicznione przez Administratora na portalu społecznościowym X (dawniej Twitter), stał się możliwy na skutek umyślnego działania Ministra Zdrowia bez uzasadnionego przepisami ustawy o systemie informacji w ochronie zdrowia celu oraz w następstwie braku odpowiednich środków bezpieczeństwa o charakterze organizacyjnym (np. procedur), które potencjalnie mogłyby temu zapobiec. Ponadto, w sposób świadomy do przekazania danych osobowych wykorzystano komunikator Whatsapp. Ponadto, Administrator pomimo faktu, że Prezes UODO poinformował go o konieczności ponownego zawiadomienia osoby, której dane dotyczą, o naruszeniu jej danych osobowych w celu przekazania wszystkich informacji wynikających z art. 34 ust. 2 w związku z art. 33 ust. 3 rozporządzenia 2016/679, nie uczynił tego w sposób prawidłowy, pozwalający na przyjęcie, iż w tym zakresie zrealizował swój obowiązek określony w tych przepisach rozporządzenia 2016/679, co wyklucza możliwość przyjęcia nieumyślności działania Administratora w tym zakresie,.

3. Działania podjęte w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą (art. 83 ust. 2 lit. c rozporządzenia 2016/679).

Administrator nie podjął żadnych innych - poza usunięciem wpisu na profilu Ministerstwa Zdrowia na platformie społecznościowej X (dawniej Twitter) - możliwych działań w tej sytuacji, jak np. przeproszenie lekarza, wyrażenie ubolewania, czy publicznego przyznania się do błędu, co mogłoby złagodzić krzywdę osoby dotkniętej naruszeniem. Jak wskazuje uchwała Sądu Najwyższego z dnia 28 czerwca 2006 r., sygn. III CZP 23/06, „Zgodnie z art. 24 k.c.[5], ten, czyje dobro zostało naruszone, może żądać m.in. aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, a w szczególności, aby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. W judykaturze oraz nauce prawa cywilnego przyjmuje się zgodnie, że treść oświadczenia może obejmować przeproszenie lub wyrażenie ubolewania, przy czym przez formę oświadczenia - zależną od okoliczności konkretnej sprawy - rozumie się sposób jego oznajmienia innym osobom lub publicznego ogłoszenia, a więc udostępnienia większej grupie nieoznaczonych osób. Nie może być wątpliwości, że unormowanie zawarte w art. 24 k.c. - stanowiące element szeroko rozumianej ochrony dóbr osobistych - osłania przede wszystkim interes osoby dotkniętej naruszeniem. Fakt ten nie może być obojętny przy rozstrzyganiu przedstawionego zagadnienia prawnego, zwłaszcza współcześnie, wobec - obserwowanego także w judykaturze - zwiększonego zagrożenia dóbr osobistych ze strony mass mediów oraz uczestników debaty publicznej, a także w związku z rozprzężeniem dobrych obyczajów zarówno w życiu prywatnym, jak i publicznym”. Powyższe wskazania przedstawione przez Sąd Najwyższy odnośnie działań mających na celu usunięcie skutków naruszenia dóbr osobistych znajdują – w ocenie Prezesa UODO – zastosowanie również w odniesieniu do czynności możliwych do podjęcia celem naprawienia szkody niemajątkowej (krzywdy) wyrządzonej naruszeniem ochrony danych osobowych.

4. Kategorie danych osobowych, których dotyczyło naruszenie (art. 83 ust. 2 lit. g rozporządzenia 2016/679).

Dane osobowe opublikowane przez Ministra Zdrowia na portalu społecznościowym X (dawniej Twitter), jak również duża część danych przetwarzanych w rejestrach, których administratorem jest Minister Zdrowia (w tym z wykorzystaniem systemu […]), stanowią dane podlegające szczególnej ochronie na gruncie art. 9 ust. 1 rozporządzenia 2016/679. Nakłada to na administratorów tych danych obowiązek szczególnego traktowania tych informacji, także z uwagi na możliwe negatywne konsekwencje dla osób, których te dane dotyczą, w przypadku ich ujawnienia osobom nieuprawnionym, włącznie z ich dyskryminacją czy też utratą dobrego imienia.

Ustalając wysokość administracyjnej kary pieniężnej, Prezes UODO nie znalazł podstaw do uwzględnienia żadnych okoliczności łagodzących mogących mieć wpływ na obniżenie ostatecznego wymiaru kary orzeczonej wobec Ministra Zdrowia.

Inne, niżej wskazane okoliczności, o których mowa w art. 83 ust. 2 rozporządzenia 2016/679, po dokonaniu oceny ich wpływu na stwierdzone w niniejszej sprawie naruszenie, zostały przez Prezesa UODO uznane za neutralne w jego ocenie, to znaczy nie mające ani obciążającego ani łagodzącego wpływu na wymiar orzeczonej administracyjnej kary pieniężnej.

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).

Prezes UODO stwierdził w niniejszej sprawie naruszenie przez Ministra Zdrowia przepisów art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679. W jego ocenie na administratorze ciąży w wysokim stopniu odpowiedzialność za niewdrożenie odpowiednich środków technicznych i organizacyjnych, które zapobiegłyby naruszeniu ochrony danych osobowych. Oczywistym jest, że w rozważanym kontekście charakteru, celu i zakresu przetwarzania danych osobowych Administrator nie „zrobił wszystkiego, czego można by było od niego oczekiwać"; nie wywiązał się tym samym z nałożonych na niego przepisami art. 25 i 32 rozporządzenia 2016/679 obowiązków.

W niniejszej sprawie okoliczność ta stanowi jednak o istocie samego naruszenia; nie jest jedynie czynnikiem wpływającym - łagodząco lub obciążająco - na jego ocenę. Z tego też względu brak odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 25 i art. 32 rozporządzenia 2016/679, nie może zostać przez Prezesa UODO uznany w niniejszej sprawie za okoliczność mogącą dodatkowo wpłynąć na surowszą ocenę naruszenia i wymiar nałożonej na Administratora administracyjnej kary pieniężnej.

2. Wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego (art. 83 ust. 2 lit. e rozporządzenia 2016/679).

Prezes UODO nie stwierdził stosownych wcześniejszych naruszeń rozporządzenia 2016/679 przez Ministra Zdrowia, w związku z czym brak jest podstaw do traktowania tej okoliczności jako obciążającej, jednakże do obowiązków każdego administratora należy przestrzeganie przepisów prawa (w tym przepisów dotyczących ochrony danych osobowych), w związku z czym brak wcześniejszych podobnych naruszeń ochrony danych osobowych nie może zostać uznany za okoliczność łagodzącą przy wymierzaniu sankcji.

3.Stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków (art. 83 ust 2 lit. f rozporządzenia 206/679).

Minister Zdrowia podjął pewne działania, które można uznać za mające na celu usunięcie skutków naruszenia; usunął wpis z profilu Ministerstwa Zdrowia na platformie X (dawniej Twitter), podjął próbę zawiadomienia lekarza, którego dane dotyczą, o naruszeniu ochrony jego danych osobowych, rozpoczął także prace nad odpowiednimi procedurami, które mają zapobiegać tego typu sytuacjom w przyszłości. Działania te nie mogą być jednak uznane za skuteczne. Minister Zdrowia nie zdołał w trakcie trwania niniejszego postępowania wdrożyć środków technicznych i organizacyjnych adekwatnych do ryzyka przetwarzania danych osobowych przy wykorzystaniu systemu [...]; nie zawiadomił również skutecznie i zgodnie w wymogami prawa osoby, której dane dotyczą, o naruszeniu ochrony jego danych osobowych. Również samo usunięcie wpisu z profilu Ministerstwa Zdrowia na platformie X – jakkolwiek spowodowało usunięcie stanu naruszenia polegającego na przetwarzaniu bez podstawy prawnej danych osobowych lekarza – nie złagodziło w istotny sposób

skutków tego naruszenia. Wielka waga naruszenia polegającego na bezprawnym publikowaniu danych osobowych w sieci Internet, a zwłaszcza w mediach społecznościowych, polega bowiem na tym, że jego negatywne skutki są natychmiastowe i praktycznie nieodwracalne. Osobie dotkniętej takim naruszeniem niezwykle trudno odzyskać kontrolę nad swoimi danymi osobowymi i wyegzekwować swoje prawo do „bycia zapomnianym" w przestrzeni internetowej. W związku z powyższym nieskuteczność (na dzień wydania niniejszej decyzji) podjętych przez Ministra Zdrowia działań mających na celu usunięcie stwierdzonych naruszeń i złagodzenia ich negatywnych skutków nie pozwala uwzględnić ich – jako okoliczność łagodzącą – przy ustaleniu wysokości orzeczonej administracyjnej kary pieniężnej.

4. Sposób w jaki organ nadzorczy dowiedział się o naruszeniu (art. 83 ust. 2 lit. h rozporządzenia 2016/679).

Prezes UODO stwierdził naruszenie przepisów rozporządzenia 2016/679 w wyniku zgłoszenia naruszenia ochrony danych osobowych dokonanego przez Administratora. Administrator dokonując tego zgłoszenia realizował jedynie ciążący na nim obowiązek prawny, brak jest podstaw do uznania, że okoliczność ta stanowi okoliczność łagodzącą. Zgodnie z Wytycznymi WP253, „Organ nadzorczy może dowiedzieć się o naruszeniu w wyniku postępowania, skarg, artykułów w prasie, anonimowych wskazówek lub powiadomienia przez administratora danych. Zgodnie z rozporządzeniem administrator ma obowiązek zawiadomić organ nadzorczy o naruszeniu ochrony danych osobowych. Zwykłe dopełnienie tego obowiązku przez administratora nie może być interpretowane jako czynnik osłabiający/łagodzący".

5. 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).

Przed wydaniem niniejszej decyzji Prezes UODO nie stosował w wobec administratora w rozpatrywanej sprawie żadnych środków wymienionych w art. 58 ust. 2 rozporządzenia 2016/679, w związku z czym administrator nie miał obowiązku podejmowania żadnych działań związanych z ich stosowaniem, a które to działania, poddane ocenie Prezesa UODO, mogłyby mieć obciążający lub łagodzący wpływ na ocenę stwierdzonego naruszenia.

6. 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).

Minister Zdrowia nie stosuje zatwierdzonych kodeksów postępowania ani zatwierdzonych mechanizmów certyfikacji, o których mowa w przepisach rozporządzenia 2016/679. Ich przyjęcie, wdrożenie i stosowanie nie jest jednak - jak stanowią przepisy rozporządzenia 2016/679 - obowiązkowe dla administratorów i podmiotów przetwarzających w związku z czym okoliczność ich niestosowania nie może być w niniejszej sprawie poczytana na niekorzyść Administratora. Na korzyść Administratora natomiast mogłaby być uwzględniona okoliczność przyjęcia i stosowania tego rodzaju

instrumentów jako środków gwarantujących wyższy niż standardowy poziom ochrony przetwarzanych danych osobowych.

7. Osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty (art. 83 ust. 2 lit. k rozporządzenia 2016/679).
Prezes UODO nie stwierdził, żeby administrator w związku z naruszeniem odniósł jakiekolwiek korzyści finansowe lub uniknął tego rodzaju strat. Brak jest więc podstaw do traktowania tej okoliczności jako obciążającej administratora. Stwierdzenie zaistnienia wymiernych korzyści finansowych wynikających z naruszenia przepisów rozporządzenia 2016/679 należałoby ocenić zdecydowanie negatywnie. Natomiast nieosiągnięcie przez administratora takich korzyści, jako stan naturalny, niezależny od naruszenia i jego skutków, jest okolicznością, która z istoty rzeczy nie może być łagodzącą dla Administratora. Potwierdza to samo sformułowanie przepisu art. 83 ust. 2 lit. k) rozporządzenia 2016/679, który nakazuje organowi nadzorczemu zwrócić należytą uwagę na korzyści „osiągnięte" – zaistniałe po stronie podmiotu dokonującego naruszenia.

8. Inne obciążające lub łagodzące czynniki (art. 83 ust. 2 lit. k rozporządzenia 2016/679).
Prezes UODO wszechstronnie rozpatrując sprawę nie odnotował innych niż opisane powyżej okoliczności mogących mieć wpływ na ocenę naruszenia i na wysokość orzeczonej administracyjnej kary pieniężnej.

Uwzględniając wszystkie omówione wyżej okoliczności, Prezes Urzędu Ochrony Danych Osobowych, uznał, iż nałożenie administracyjnej kary pieniężnej na Ministra Zdrowia jest konieczne i uzasadnione wagą, charakterem oraz zakresem zarzucanych Administratorowi naruszeń przepisów rozporządzenia 2016/679. Stwierdzić należy, iż zastosowanie wobec Ministra Zdrowia jakiegokolwiek innego środka naprawczego przewidzianego w art. 58 ust. 2 rozporządzenia 2016/679, w szczególności zaś poprzestanie na upomnieniu (art. 58 ust. 2 lit. b), nie byłoby proporcjonalne do stwierdzonych nieprawidłowości w procesie przetwarzania danych osobowych oraz nie gwarantowałoby tego, że Administrator w przyszłości nie dopuści się kolejnych zaniedbań. Uzasadniając fakt nałożenia na Ministra Zdrowia maksymalnej dopuszczalnej dla podmiotów sektora finansów publicznych administracyjnej kary pieniężnej (100 000 zł), wskazać należy, że w ocenie Prezesa UODO kara w niższej wysokości nie spełniłaby swojej funkcji odstraszającej, o której m.in. wprost jest mowa w art. 83 ust. 1 rozporządzenia 2016/670; nie zdyscyplinowałaby też Administratora do prawidłowej współpracy z Prezesem UODO w przyszłości (ajak wskazano niżej kara nałożona w tej konkretnej sprawie ma też charakter dyscyplinujący i prewencyjny). W tym miejscu należy zaznaczyć, że nie można mówić w niniejszej sprawie o surowości kary ograniczonej limitem 100 000 zł, w związku z czym wymierzenie kary nawet w maksymalnym wymiarze tego zagrożenia nie stanowi surowej sankcji. Warto również podkreślić, że wysokość orzeczonej kary wynika wyłącznie z radykalnego (w stosunku do ogólnych zagrożeń karą pieniężną przewidzianą przepisami rozporządzenia 2016/679) ograniczenia zagrożenia przewidzianego dla podmiotów publicznych w art. 102 ust. 1 u.o.d.o. Gdyby kara pieniężna wymierzana była w ramach ogólnego, określonego w art. 83 ust. 5 rozporządzenia

2016/679, zagrożenia karą pieniężną (bez uwzględnienia ograniczenia z art. 102 ust. 1 u.o.d.o.), kara orzeczona w niniejszej sprawie – ze względu na dużą wagę i naganny charakter naruszenia (co wskazano w uzasadnieniu zaskarżonej decyzji) – musiałaby być wymierzona w kwocie wielokrotnie przekraczającej kwotę 100 000 zł. Na zasadach ogólnych maksymalne zagrożenie karą za naruszenie zasad dotyczących przetwarzania danych osobowych określonych w art. 5 rozporządzenia 2016/679 oraz art. 6 i 9 rozporządzenia 2016/679 - zgodnie z art. 83 ust. 5 lit. a) rozporządzenia 2016/679 – wynosi 20 000 000 EUR.

Odnosząc się do wysokości wymierzonej Ministrowi Zdrowia administracyjnej kary pieniężnej, wskazać należy, że – wobec faktu, iż Administrator jest jednostką sektora finansów publicznych, o której mowa w art. 9 pkt 1) ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r., poz. 1270 ze zm.) – zastosowanie znajdzie art. 102 ust. 1 pkt 1) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), z którego wynika ograniczenie wysokości (do 100.000 zł) administracyjnej kary pieniężnej, jaka może zostać nałożona na jednostkę sektora finansów publicznych.

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. będzie w tym indywidulanym przypadku skuteczna, proporcjonalna i odstraszająca.

Zdaniem Prezesa UODO nałożona na Ministra Zdrowia administracyjna kara pieniężna będzie skuteczna, albowiem doprowadzi do stanu, w którym Administrator stosował będzie takie środki techniczne i organizacyjne, które zapewnią przetwarzanym danym stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą oraz wadze zagrożeń towarzyszącym procesom przetwarzania tych danych osobowych, a także będzie przetwarzał dane przy wykorzystaniu systemu [...] zgodnie z celami określonymi w ustawie o systemie informacji w ochronie zdrowia, co zapewni jednocześnie zgodność tych działań z przepisami prawa. Skuteczność tej kary równoważna jest zatem gwarancji tego, iż Minister Zdrowia od momentu zakończenia niniejszego postępowania będzie ze starannością podchodzić do wymogów stawianych przez przepisy o ochronie danych osobowych.

Zastosowana administracyjna kara pieniężna jest również proporcjonalna do stwierdzonego naruszenia przepisów rozporządzenia 2016/679, w tym zwłaszcza jego wagi, negatywnego skutku dla osoby dotkniętej ochroną danych osobowych oraz wysokiego ryzyka negatywnych konsekwencji jakie, w związku z naruszeniem polegającym na braku środków technicznych i organizacyjnych adekwatnych do ryzyka przetwarzania danych osobowych przy wykorzystaniu systemu [...], mogą ponieść osoby, których dane w tym systemie są przetwarzane. Zdaniem Prezesa UODO, nałożona na Ministra Zdrowia administracyjna kara pieniężna nie jest dla niego nadmiernie dotkliwa, wobec ustawowego ograniczenia jej wysokości w przypadku jednostek sektora finansów publicznych. W szczególności jej zapłata nie wpłynie na zdolność Ministra Zdrowia do wywiązywania się przez

niego z jego ustawowych zadań. Zdaniem Prezesa UODO, Administrator powinien i jest w stanie ponieść konsekwencje swoich zaniedbań w sferze ochrony danych, stąd nałożenie kary w wysokości 100 000 złotych (słownie: stu tysięcy złotych) jest w pełni uzasadnione.

W ocenie Prezesa UODO, administracyjna kara pieniężna spełni w tych konkretnych okolicznościach funkcję edukacyjną ale i prewencyjną; w ocenie Prezesa UODO wskaże bowiem zarówno Ministrowi Zdrowia, jak i innym administratorom danych, na naganność lekceważenia obowiązków administratorów związanych z zaistnieniem naruszenia ochrony danych osobowych, jak również na odpowiedzialność organów władzy państwowej za bezprawne działania podejmowane przez nie z wykorzystaniem swojej władzy oraz możliwości, które ta władza daje.

W ocenie Prezesa UODO, zastosowana administracyjna kara pieniężna spełnia w ustalonych okolicznościach niniejszej sprawy przesłanki, o których mowa w art. 83 ust. 1 rozporządzenia 2016/679, ze względu na wagę stwierdzonych naruszeń w kontekście podstawowych wymogów i zasad rozporządzenia 2016/679 - zwłaszcza zasady zgodności z prawem, rzetelności i przejrzystości oraz zasady integralności i poufności wyrażonych w art. 5 ust. 1 lit. a) i f) rozporządzenia 2016/679.

Celem nałożonej kary jest doprowadzenie do przestrzegania przez Ministra Zdrowia w przyszłości przepisów rozporządzenia 2016/679.

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

[1] „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się".

[2] „1.Każdy ma prawo do ochrony danych osobowych, które go dotyczą. 2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. 3. Przestrzeganie tych zasad podlega kontroli niezależnego organu"

[3] decyzja w języku angielskim dostępna pod adresem: https://edpb.europa.eu/system/files/2023-01/final_adoption_version_decision_wa_redacted_1.pdf

[4] Wytyczne Europejskiej Rady Ochrony Danych nr 9/2022, przyjęte 28 marca 2023 r.

[5] Ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny (Dz.U. z 2023 r. poz. 1610 ze zm.)