



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 31 sierpnia 2009 r.

DIS/DEC- 877/31613/09

dot. DIS-K-421/43/09

D E C Y Z J A

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 36, art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), oraz § 4, § 5 pkt 8, § 7 ust. 1 pkt 1 i pkt 2, § 7 ust. 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez CM Sp. z o.o. Niepubliczny Zakład Opieki Zdrowotnej z siedzibą w (...),

I. Nakazuję CM Sp. z o.o. Niepublicznemu Zakładowi Opieki Zdrowotnej z siedzibą w (...), usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. Zabezpieczenie danych osobowych pacjentów Centrum Medyczne

Sp. z o.o. Niepublicznego Zakładu Opieki Zdrowotnej z siedzibą w (...) (w tym danych osobowych Pana X) przetwarzanych, przy użyciu urządzenia densytometrycznego typu Prodygy enCorenr 63354/13422, przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem w terminie 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.

- 2. Opracowanie i wdrożenie polityki bezpieczeństwa, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 3. Uzupełnienie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, o procedury opisujące sposób wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych – w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 4. Przedłożenie dokumentu potwierdzającego wyznaczenie administratora bezpieczeństwa informacji – w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 5. Zapewnienie, aby system informatyczny o nazwie „Q-Klinika 3000” (służący do przetwarzania danych osobowych pacjentów), dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym, odnotowywał datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu - w terminie 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 6. Zapewnienie, aby system informatyczny o nazwie „Q-Klinika 3000” (służący do przetwarzania danych osobowych pacjentów), dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym umożliwiał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu - w terminie 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**

Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w CM Sp. z o.o. Niepublicznym Zakładzie Opieki Zdrowotnej z siedzibą w (...) (sygn. akt....), zwaną dalej także Centrum Medycznym, w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. ustawą z dnia 29 sierpnia 1997 r.

o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwaną dalej ustawą oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024), zwanym dalej

rozporządzeniem. W toku kontroli odebrano od Dyrektora Medycznego i pracowników Centrum Medycznego ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli (sygn. akt ...), który został podpisany przez Dyrektora Zarządzającego i Dyrektora Finansowego Centrum Medycznego.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Centrum Medyczne, jako administrator danych, naruszyło przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niezabezpieczeniu danych osobowych pacjentów Centrum Medycznego (w tym danych osobowych Pana X) przetwarzanych, przy użyciu urządzenia densytometrycznego typu Prodygy enCore nr 63354/13422, przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Nieopracowaniu i niewdrożeniu polityki bezpieczeństwa.
3. Niezawarcia w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, procedur opisujących sposób wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.
4. Niewyznaczeniu administratora bezpieczeństwa informacji.
5. Niezapewnieniu, aby system informatyczny o nazwie „Q-Klinika 3000” (służący do przetwarzania danych osobowych pacjentów), dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym, odnotowywał datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu.
6. Niezapewnieniu, przez system informatyczny o nazwie „Q-Klinika 3000” (służący do przetwarzania danych osobowych pacjentów), dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane do systemu.

W piśmie z dnia 2 czerwca 2009 r. (sygn....), stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Centrum Medyczne zostało poinformowane o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji o prawie wypowiedzenia się co do zebranych dowodów i materiałów.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Zarządzający i Dyrektor Finansowy Centrum Medycznego, pismami z dnia 29 czerwca 2009 r. i z dnia 17 lipca 2009 r., przesłali wyjaśnienia w zakresie stwierdzonych uchybień.

Ze złożonych wyjaśnień wynika, iż:

1. Urządzenie densytometryczne typu Prodygy Encore nr 63354/13422 było dzierżawione przez Centrum Medyczne, a jego obsługa została zlecona firmie Laboratorium Y Sp. z o.o. z siedzibą w (...), reprezentowanej przez Pana Z. Urządzenie to znajdowało się w siedzibie Centrum Medycznego do miesiąca lutego 2007 r., następnie zostało ono zdemontowane. Podmiotem wyłącznie uprawnionym do korzystania z pomieszczenia, w którym znajdowało się to urządzenie był zleceniobiorca tj. Y Sp. z o.o. z siedzibą w (...). Pracownicy Centrum Medycznego nie byli przeszkoleni i uprawnieni do obsługi tego urządzenia, dlatego też nie usunęli danych osobowych pacjentów Centrum Medycznego z ww. urządzenia. Po demontażu tego urządzenia wszystkie dane (w tym dane pacjentów, którzy w Centrum Medycznym poddani zostali temu badaniu) powinny zostać usunięte przez faktycznego operatora urządzenia, czyli firmę Laboratorium Y Sp. z o.o. z siedzibą w (...).
2. Trwają prace nad aktualizacją dokumentu o nazwie „Polityka bezpieczeństwa”. Planowany termin dokonania aktualizacji ww. dokumentu przewidywany jest na dzień 31 sierpnia 2009 r.
3. Rozpoczęto prace nad aktualizacją dokumentu o nazwie „Instrukcja dla systemów informatycznych przetwarzających dane osobowe”. Planowany termin zaktualizowania ww. dokumentu przewidywany jest na dzień 31 sierpnia 2009 r.
4. Wyznaczony został administrator bezpieczeństwa informacji.
5. W trakcie realizacji jest usuwanie uchybień dotyczących funkcjonalności systemu informatycznego o nazwie „Q-Klinika 3000” (służącego do przetwarzania danych osobowych pacjentów).

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

Zgodnie z art. 36 ust. 1 ustawy administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabránieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Jak ustalono w toku kontroli badanie densytometryczne Pana X, zostało przeprowadzone w Centrum Medycznym w dniu 11 października 2004 r. Zarówno badanie jak i jego opis zostało wykonane przez Pana Z lekarza chorób wewnętrznych. Badanie to zostało przeprowadzone za pomocą urządzenia densytometrycznego typu Prodygy Encore nr 63354/13422. Urządzenie to było użytkowane w Centrum Medycznym na podstawie umowy dzierżawy zawartej w dniu 25 stycznia 2002 r. pomiędzy Centrum Medycznym,

a Firmą S PPH z siedzibą w (...) – (...), reprezentowaną przez Pana Z. Ponadto, jak wyjaśniła Dyrektor Medyczny Centrum Medycznego, urządzenie to zostało zdemontowane w miesiącu lutym 2007 r. natomiast, przed jego demontażem dane pacjentów zostały usunięte i na tę okoliczność został sporządzony protokół usunięcia danych. Jednak w toku czynności kontrolnych nie przedłożono do wglądu dokumentu potwierdzającego wykonanie czynności, o których mowa powyżej. Dokumentu tego do dnia dzisiejszego nie przesłano również do siedziby Biura Generalnego Inspektora Ochrony Danych Osobowych w Warszawie, pomimo iż w toku czynności kontrolnych Dyrektor Medyczny Centrum Medycznego zobowiązała się, iż protokół usunięcia danych zostanie przesłany do siedziby Biura Generalnego Inspektora Ochrony Danych Osobowych w terminie do dnia 17 marca 2009 r.

Nadmienić ponadto należy, iż w toku kontroli (DIS-K-...) przeprowadzonej u Pana Z prowadzącego działalność gospodarczą pod nazwą „Laboratorium Y Z” z siedzibą w (...), ustalono, iż przedmiotowe urządzenie densytometryczne w Centrum Medycznym zostało w dniu 9 lutego 2007 r. zdemontowane przez autoryzowanego dystrybutora firmy General Electric z siedzibą w (...). Następnie urządzenie to (wraz z danymi pacjentów Centrum Medycznego - w tym danymi osobowymi Pana X), zostało przeniesione do Niepublicznego Zakładu Opieki Zdrowotnej KL z siedzibą w (...). Wobec powyższego należy stwierdzić, iż nie nastąpiło usunięcie danych osobowych pacjentów Centrum Medycznego pozyskanych za pomocą urządzenia densytometrycznego typu Prodygy Encore nr 63354/13422.

Jednocześnie pismem z dnia 29 czerwca 2009 r., stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Zarządzający i Dyrektor Finansowy Centrum Medycznego poinformowali, iż urządzenie densytometryczne typu Prodygy Encore nr 63354/13422 było dzierżawione przez Centrum Medyczne, a jego obsługa była zlecona firmie Laboratorium Y Sp. z o.o. z siedzibą w (...), reprezentowanej przez Pana Z. Urządzenie to znajdowało się w siedzibie Centrum Medycznego do miesiąca lutego 2007 r. Wyłącznie uprawnionym do korzystania z pomieszczenia w którym stało to urządzenie był zleceniobiorca tj. Y Sp. z o.o. z siedzibą w (...). Pracownicy Centrum Medycznego nie byli przeszkoleni i uprawnieni do obsługi tego urządzenia, dlatego też nie usunęli danych osobowych pacjentów Centrum Medycznego z ww. urządzenia.

Po demontażu tego urządzenia Centrum Medyczne uważało, iż wszystkie dane pacjentów, którzy w Centrum Medycznym poddani zostali temu badaniu, zostaną usunięte przez faktycznego operatora urządzenia, czyli firmę Laboratorium Y Sp. z o.o. z siedzibą w (...).

Odnosząc się do ww. wyjaśnień należy podkreślić, iż sam fakt, że pracownicy Centrum Medycznego nie byli przeszkoleni i uprawnieni do obsługi przedmiotowego urządzenia, nie zwalnia administratora danych od odpowiedzialności związanej z brakiem zabezpieczenia

danych osobowych pacjentów (w tym danych osobowych Pana X) przetwarzanych, przy użyciu ww. urządzenia.

Ponadto, należy zauważyć, iż badanie densytometryczne Pana X, zostało przeprowadzone w Centrum Medycznym w dniu 11 października 2004 r. Badanie to wykonane zostało na podstawie umowy zlecenia Nr 0016/2002 zawartej w dniu 1 lutego 2002 r. pomiędzy Centrum Medycznym, a Panem Z zamieszkałym w (...), zwanym Zleceniobiorcą. Przedmiotem zawartej umowy było m.in. wykonywanie przez Zleceniobiorcę badań diagnostycznych na rzecz pacjentów Centrum Medycznego. Na podstawie zawartej umowy, Centrum Medyczne zobowiązane było m. in. do zapewnienia obsługi związanej z rejestracją pacjenta i rozliczeniem należności, jak również do ewidencjonowania i przechowywania dokumentacji lekarskiej.

W ocenie Generalnego Inspektora Ochrony Danych Osobowych, już z datą rozwiązania ww. umowy zlecenia tj. z dniem 30 września 2006 r. Centrum Medyczne powinno spowodować, aby dane osobowe pacjentów, które pozyskane zostały w związku z realizacją ww. umowy (w tym dane osobowe Pana X), zostały odpowiednio zabezpieczone poprzez zapisanie ich na inny nośnik elektroniczny w celu zapewnienia dostępności do tych danych wyłącznie osobom uprawnionym. Ponadto, na podstawie pozyskanego materiału dowodowego wynika jednoznacznie, iż Centrum Medyczne nawet, po rozwiązaniu umowy o współpracy zawartej w dniu 31 stycznia 2006 r. z Laboratorium Y Sp. z o.o. z siedzibą w (...), jak i po rozwiązaniu umowy o współpracy zawartej w dniu 1 października 2006 r. z Panem Z prowadzącym działalność gospodarczą pod nazwą „Laboratorium Y Z” i w konsekwencji demontażem przedmiotowego urządzenia, nie podjęło stosownych działań w celu zabezpieczenia danych osobowych swoich pacjentów pozyskanych w związku z realizacją ww. umów.

Biorąc powyższe pod uwagę należy stwierdzić, iż Centrum Medyczne nie zastosowało odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych pacjentów (w tym danych osobowych Pana X) przetwarzanych, przy użyciu urządzenia densytometrycznego typu Prodygy enCore nr 63354/13422, a tym samym nie zabezpieczyło danych osobowych swoich pacjentów, przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zgodnie z art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. W myśl § 3 ust. 1 rozporządzenia, na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zgodnie z ust. 2, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w

formie pisemnej. Natomiast, zgodnie z ust. 3, dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

W toku czynności kontrolnych ustalono, iż w Centrum Medycznym nie została opracowana polityka bezpieczeństwa, o której mowa w § 3 ust. 1 rozporządzenia.

Natomiast jak wynika z treści pisma z dnia 29 czerwca 2009 r., stanowiącego odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, Centrum Medyczne posiada dokument o nazwie „Polityka bezpieczeństwa”, lecz aktualnie dokument ten jest aktualizowany i dopiero po jego aktualizacji zostanie przesłany do Biura Generalnego Inspektora Ochrony Danych Osobowych.

Biorąc powyższe pod uwagę, Centrum Medyczne jest zobowiązane do przywrócenia stanu zgodnego z prawem, w zakresie opracowania i wdrożenia dokumentu o nazwie „Polityka bezpieczeństwa”.

Zgodnie z § 5 pkt 8 rozporządzenia, instrukcja zarządzania systemem informatycznym, o której mowa w § 3 ust. 1 rozporządzenia, zawiera w szczególności, procedury opisujące wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Przedstawiony w toku kontroli dokument o nazwie „Zabezpieczenie systemów informatycznych CDM” nie zawiera w swej treści informacji, o których mowa powyżej.

Pismem z dnia 17 lipca 2009 r., stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Zarządzający i Dyrektor Finansowy Centrum Medycznego poinformowali, iż trwają prace nad modyfikacją dokumentu o nazwie „Instrukcja dla systemów informatycznych przetwarzających dane osobowe”. Planowany termin zakończenia aktualizacji ww. dokumentu przewidywany jest na dzień 31 sierpnia 2009 r.

Biorąc powyższe pod uwagę, Centrum Medyczne jest zobowiązane do przywrócenia stanu zgodnego z prawem, w zakresie uzupełnienia dokumentu o nazwie „Instrukcja dla systemów informatycznych przetwarzających dane osobowe”, o informacje o których mowa w § 5 pkt 8 rozporządzenia.

Zgodnie z art. 36 ust. 3 ustawy, administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

W toku czynności kontrolnych nie przedłożono do wglądu dokumentu potwierdzającego wyznaczenie administratora bezpieczeństwa informacji. Dokument ten, do dnia dzisiejszego nie został przesłany do siedziby Biura Generalnego Inspektora Ochrony Danych Osobowych w Warszawie pomimo, iż w toku kontroli Dyrektor Medyczny Centrum Medycznego

zobowiązała się, iż kserokopia tego dokument zostanie do dnia 17 marca 2009 r. przesłana do Biura Generalnego Inspektora Ochrony Danych Osobowych.

Natomiast pismem z dnia 29 czerwca 2009 r., stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Zarządzający i Dyrektor Finansowy Centrum Medycznego poinformowali, iż wyznaczony został administrator bezpieczeństwa informacji.

Z uwagi jednak na to, że nie przesłano na tą okoliczność dowodu potwierdzającego, wyznaczanie administratora bezpieczeństwa informacji, nie można uznać, iż przywrócony został w tym zakresie stan zgodny z prawem.

Zgodnie z art. 38 ustawy, administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Natomiast zgodnie z § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie: 1) daty pierwszego wprowadzenia danych do systemu; 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba, że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

W toku kontroli ustalono, iż w odniesieniu do systemu informatycznego o nazwie „Q-Klinika 3000” (służącego do przetwarzania danych osobowych pacjentów), nie została zapewniona kontrola nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone.

Ponadto, ustalono, że ww. system informatyczny (w przypadku importu danych z listy) nie zapewnia dla każdej osoby, której dane osobowe są przetwarzane w tym systemie, odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane do systemu.

Zgodnie z § 7 ust. 3 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system ten zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia.

W toku czynności kontrolnych ustalono, że system informatyczny o nazwie „Q-Klinika 3000” nie zapewnia dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje w zakresie daty pierwszego wprowadzenia danych do systemu informatycznego oraz identyfikatora użytkownika wprowadzającego dane do systemu.

Pismem z dnia 29 czerwca 2009 r., stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Zarządzający i Dyrektor Finansowy Centrum Medycznego poinformowali, iż trwają prace w zakresie modyfikacji systemu informatycznego o nazwie „Q-Klinika 3000” (służącego do przetwarzania danych osobowych pacjentów).

W związku z tym uznać należy, że uchybienia we wskazanym wyżej zakresie nie zostały usunięte, a zatem wyznaczony został odpowiedni termin do przywrócenia w ww. zakresie stanu zgodnego z prawem.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja jest ostateczna. Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych oraz art. 129 § 2 Kodeksu postępowania administracyjnego, strona niezadowolona z niniejszej decyzji może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: ul. Stawki 2, 00-193 Warszawa) z wnioskiem o ponowne rozpatrzenie sprawy, w terminie 14 dni od dnia doręczenia niniejszej decyzji.