



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*Michał Serzycki*

Warszawa, dnia 23 stycznia 2008 r.

DIS/DEC- 51/1641/08

dot. [...]

**D E C Y Z J A**

Na podstawie art. 104 § 1 i art. 105 § 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 ust. 1 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 pkt 3, pkt 4, pkt 5, § 5 pkt 7, § 7 ust. 1 pkt 1, pkt 2, pkt 4, § 7 ust. 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. z 2004 r., Nr 100, poz. 1024) i częścią A pkt II ust. 2 lit. a i lit. b, częścią A pkt III ppkt 1, częścią A pkt IV ust. 2, częścią B pkt VIII załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Samodzielny Zespół Publicznych Zakładów Opieki Zdrowotnej w W.,

**I. Nakazuję Samodzielnemu Zespołowi Publicznych Zakładów Opieki w W. uchybień w procesie przetwarzania danych osobowych, poprzez:**

- 1. Uzupelnienie polityki bezpieczeństwa o opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami, określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

2. **Zmodyfikowanie systemu informatycznego o nazwie „A” służącego do prowadzenia obsługi kadrowo - płacowej pracowników tak, aby dla każdej osoby, której dane są przetwarzane w tym systemie informatycznym, system zapewniał odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu, w terminie 6 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
3. **Zmodyfikowanie systemu informatycznego o nazwie „B” służącego do przetwarzania danych osobowych pacjentów [...] tak, aby dla każdej osoby, której dane są przetwarzane w tym systemie informatycznym, system zapewniał odnotowanie identyfikatora użytkownika wprowadzającego dane osobowe do systemu, w terminie 6 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Zmodyfikowanie systemu informatycznego o nazwie „A” służącego do prowadzenia obsługi kadrowo - płacowej pracowników tak, aby odnotowanie daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu następowało automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych w systemie, w terminie 6 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
5. **Zmodyfikowanie systemu informatycznego o nazwie „B” służącego do przetwarzania danych osobowych pacjentów [...] tak, aby odnotowanie daty pierwszego wprowadzenia danych do systemu następowało automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych w systemie, w terminie 6 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
6. **Zmodyfikowanie systemu informatycznego o nazwie „A” służącego do prowadzenia obsługi kadrowo - płacowej pracowników tak, aby dla każdej osoby, której dane są przetwarzane w tym systemie informatycznym, system umożliwiał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia, w terminie 6 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
7. **Używania do systemów informatycznych o nazwach: „C” służącego do rejestrowania danych osobowych pacjentów wraz z historią choroby, „B” służącego do przetwarzania danych osobowych pacjentów [...] oraz „A” służącego do prowadzenia obsługi kadrowo - płacowej pracowników, hasła składającego się co najmniej z 8 znaków, zawierającego małe i wielkie litery oraz cyfry lub znaki specjalne, w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**

**II. W pozostałym zakresie postępowanie umarzam.**

## Uzasadnienie

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę (sygn. akt [...]) w Samodzielnym Zespole Publicznych Zakładów Opieki Zdrowotnej w W. (dalej: SZPZOZ [...]), 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 pracowników SZPZOZ [...] ustne wyjaśnienia, skontrolowano systemy informatyczne służące do przetwarzania danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Dyrektora SZPZOZ [...].

Na podstawie zgromadzonego w toku kontroli materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych, SZPZOZ [...], jako administrator danych osobowych naruszył przepisy o ochronie danych osobowych. Stwierdzono następujące uchybienia:

1) brak zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności nie zabezpieczono danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, gdyż bieżąca dokumentacja medyczna (historie choroby pacjentów hospitalizowanych na O.) była przechowywana w pokoju lekarskim, w niezamykanym pudełku stojącym na biurku (art. 36 ust. 1 ustawy),

2) polityka bezpieczeństwa nie spełnia wymogów określonych w § 4 pkt 3, pkt 4, pkt 5 rozporządzenia, gdyż nie zawiera w treści: opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi, opisu sposobu przepływu danych pomiędzy poszczególnymi systemami, a także określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,

3) „Instrukcja zarządzania systemami informatycznymi” w SZPZOZ [...] nie zawierała opisu sposobu realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia, tj. informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia (§ 5 pkt 7 rozporządzenia),

4) systemy informatyczne o nazwach „B” i „A” nie zapewniały odnotowania daty pierwszego wprowadzenia danych do systemu, identyfikatora użytkownika wprowadzającego dane osobowe do

systemu, informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia (§ 7 ust. 1 pkt 1, pkt 2, pkt 4 rozporządzenia),

5) brak automatycznego odnotowywania daty pierwszego wprowadzenia danych do systemów informatycznych „B” i „A” i identyfikatora użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 2 rozporządzenia),

6) systemy informatyczne o nazwach „B” i „D” i „A” nie zapewniały sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji, o których mowa w § 7 ust. 1 rozporządzenia (§ 7 ust. 3 rozporządzenia),

7) użytkownicy systemu informatycznego o nazwie „B” nie posiadali odrębnych identyfikatorów, a dostęp do danych w tym systemie jest uzyskiwany bez konieczności wprowadzania identyfikatora i hasła (część A pkt II ust. 2 lit. a i lit. b załącznika do rozporządzenia),

8) brak zainstalowanego na stacji roboczej systemu informatycznego o nazwie „A” służącego do prowadzenia obsługi kadrowo-płacowej pracowników SZPZOZ [...], oprogramowania antywirusowego, na serwerze systemu informatycznego o nazwie „C” służącego do rejestrowania danych osobowych pacjentów SZPZOZ [...] wraz z historią choroby, nie zainstalowano oprogramowania antywirusowego (część A pkt III ppkt 1),

9) zmiana hasła dostępu do systemu informatycznego „D” służącego do ewidencji osób [...] następowała rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia),

10) hasła uwierzytelniające użytkowników systemów informatycznych „C”, „D”, „E”, „B” oraz „A” nie składały się co najmniej z 8 znaków, hasła nie zawierały małych i wielkich liter oraz cyfr lub znaków specjalnych (część B pkt VIII załącznika do rozporządzenia).

W związku z powyższym w dniu [...] listopada 2007 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w celu wyjaśnienia okoliczności sprawy (pismo znak: [...]).

W odpowiedzi na zawiadomienie o wszczęciu postępowania Dyrektor Samodzielnego Zespołu Publicznych Zakładów Opieki Zdrowotnej [...] pismem z dnia [...] grudnia 2007 r. (znak: [...]) złożył wyjaśnienia, w których poinformował, m.in., że:

1) zobowiązano Ordynatora Oddziału i lekarzy do realizacji postanowień art. 36 ust. 1 ustawy w zakresie przechowywania bieżącej dokumentacji medycznej w pokoju lekarskim. Obecnie dokumentacja medyczna przechowywana jest w zamkniętych szafach i nie jest dostępna osobom nieupoważnionym,

2) program „D” to program narzucony przez Narodowy Fundusz Zdrowia (dalej: NFZ) i producent nie udostępnia opisu programu. Program ten ma zostać zastąpiony od 2008 r. przez system „F”; wysłano prośbę do producenta systemu informatycznego „B” o udostępnienie opisu struktury danych; system „C” od 2008 r. zostanie zastąpiony systemem „F”; system „E” służy wymianie danych z NFZ i w gestii NFZ jest jego dokumentacja; system „F” – jest nowym

systemem służącym do obsługi [...], którego wdrożenie ma nastąpić w terminie do dnia [...] stycznia 2008 r.,

3) dane osobowe przetwarzane przez SZPZOZ [...] są udostępniane: osobom, których dane dotyczą; Narodowego Funduszu Zdrowia na podstawie zawartej umowy; organom państwowym lub organom samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem; wymienione podmioty nie stanowią odbiorców w rozumieniu art. 7 pkt 6 ustawy,

4) został zakupiony nowy sprzęt z systemem operacyjnym „G”, który zostanie podłączony do domeny i autentyfikacja w systemie „B” będzie kontrolowana przez serwer; została wskazana jedna osoba upoważniona do obsługi systemu informatycznego „B”,

5) nowy system „F”, który zastąpi system „D”, nie wymusza na użytkowniku zmiany hasła co 30 dni; w związku z powyższym został zgłoszony postulat do producenta, a do czasu odniesienia się do niego użytkownicy systemu zostaną zobowiązani do zmiany hasła co 30 dni wewnętrzną instrukcją,

6) został zakupiony nowy serwer z systemem „H” i program antywirusowy do serwera; pełne wdrożenie nastąpi w terminie do [...] stycznia 2008 r.; we wrześniu 2007 r. na stacji roboczej systemu „A” został zainstalowany program antywirusowy,

7) do dnia [...] stycznia 2008 r. wszystkie stacje robocze zostaną wymienione na nowe z systemem operacyjnym „G” pod kontrolą domeny serwera „H” i zostanie wdrożona właściwa polityka haseł: minimum 8 znaków, minimum jedna duża litera, minimum jedna cyfra lub znak specjalny, ważność 30 dni, historia ostatnich 6 haseł,

8) w systemie „B” jest rejestrowana data wprowadzenia danych, system jest obsługiwany przez jedną osobę i dane nie są udostępniane,

9) przejście na system spełniający określone warunki, wymaga pozyskania środków finansowych, przeprowadzenie przetargu oraz wdrożenie tego systemu; w związku z tym postulat zapewnienia odnotowania informacji, o których mowa w § 7 ust. 1 pkt 1, pkt 2 i pkt 4 rozporządzenia, może zostać zrealizowany nie wcześniej, niż w dniu [...] lipca 2008 r.,

10) system „D” zostanie zastąpiony przez system „F”, w którym istnieje możliwość uzyskania informacji o dacie wprowadzenia, modyfikacji i przekazywaniu danych oraz identyfikatorze użytkownika; w systemie „B” gromadzone są następujące dane: imię i nazwisko, wiek, płeć, wykres będący wynikiem badania. Dane te nie są modyfikowane, a data ich wprowadzenia jest rejestrowana. Dane powyższe nie są przekazywane, więc raport zawiera jedynie datę ich wprowadzenia.

Do ww. pisma załączono dowody w postaci kopii pisma z dnia [...] grudnia 2007 r. (znak: [...]) skierowanego do M. Sp. z o.o., oraz pismo z dnia [...] grudnia 2007 r. (znak: [...]) skierowanego do K.

Ponadto, pismem z dnia [...] stycznia 2008 r. Samodzielny Zespół Publicznych Zakładów Opieki Zdrowotnej [...] poinformował, że został wycofany z użytkowania system „D”, hasła do systemów „C”, „B” i „A” nie zawierają małych i wielkich liter oraz cyfr i znaków specjalnych, natomiast wymogi takie spełniają hasła do systemu „E”. Do powołanego pisma załączono wydruk z systemu informatycznego „E” obrazujący spełnienie wymogów dotyczące hasła (hasło ośmioznakowe zawierające małe i wielkie litery oraz cyfry i opcjonalnie znaki specjalne) oraz wydruk z systemu informatycznego o nazwie „C” potwierdzający zainstalowanie programu antywirusowego.

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

Zgodnie z § 4 rozporządzenia polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:

- 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- 3) opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- 4) sposób przepływu danych pomiędzy poszczególnymi systemami;
- 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

W toku postępowania ustalono, iż jest prowadzona dokumentacja opisująca sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. polityka bezpieczeństwa Samodzielnego Zespołu Publicznych Zakładów Opieki Zdrowotnej. Powołany dokument wdrożony został przez administratora danych jednak nie spełnia wymogów, o których mowa w § 4 pkt 3 rozporządzenia, gdyż nie zawiera w treści: opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Zgodnie z § 7 ust. 1 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym 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;
- 3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;

4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba, że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

W toku czynności kontrolnych ustalono, że system informatyczny o nazwie „A” służący do prowadzenia obsługi kadrowo - płacowej pracowników nie zapewnia odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu, natomiast system informatyczny o nazwie „B” służący do przetwarzania danych osobowych pacjentów [...], nie zapewnia odnotowania identyfikatora użytkownika wprowadzającego dane osobowe do systemu.

Zgodnie z § 7 ust. 2 rozporządzenia, odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2 rozporządzenia, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

Odnnotowanie daty pierwszego wprowadzenia danych do systemu informatycznego o nazwie „A” i identyfikatora użytkownika wprowadzającego dane osobowe do tego systemu nie następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych w systemie; odnotowanie daty pierwszego wprowadzenia danych do systemu informatycznego o nazwie „B” nie następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

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

W toku postępowania ustalono, że system informatyczny „A” nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji, o których mowa w § 7 ust. 1 rozporządzenia.

Zgodnie z częścią B pkt VIII załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

W toku czynności kontrolnych ustalono, że dla „systemów informatycznych o nazwach: „C”, „B” oraz „A” hasło do uwierzytelniania użytkowników nie składa się co najmniej z 8 znaków. Hasło nie zawiera małych i wielkich liter oraz cyfr lub znaków specjalnych.

Generalny Inspektor uwzględniając wyjaśnienia strony dotyczące podjęcia działań zmierzających do modyfikacji systemu informatycznego o nazwie „B” w zakresie zapewnienia odnotowania informacji, o których mowa w § 7 ust. 1 pkt 2 oraz automatycznego odnotowywania tych informacji, oraz systemu informatycznego o nazwie „A” w zakresie zapewnienia odnotowania informacji, o których mowa w § 7 ust. 1 pkt 1 i pkt 2, a także umożliwienia sporządzenia i wydrukowania raportu zawierającego informacje, o których mowa w § 7 ust. 1, oraz

automatycznego odnotowywania tych informacji przez systemy informatyczne „B” i „A”, wyznaczył sześciomiesięczny termin wykonania niniejszej decyzji. Jednocześnie w związku ze złożeniem przez stronę oświadczenia, iż do dnia [...] stycznia 2008 r. nie została wdrożona polityka haseł składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne w odniesieniu do następujących systemów: „C”, „B” i „A” (mimo wcześniejszego wskazania, że uchybienia zostaną usunięte do dnia [...] stycznia 2008 r.), organ wyznaczył miesięczny termin do wykonania decyzji w tym zakresie.

Stosowanie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiegokolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Przesłanką umorzenia postępowania na podstawie art. 105 § 1 k.p.a. jest bezprzedmiotowość postępowania „z jakiegokolwiek przyczyny”, czyli każdej przyczyny powodującej brak jednego z elementów materialnoprawnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z 21 stycznia 1999 r. SA/Sz 1029/97).

W toku postępowania zostały usunięte pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, poprzez:

1) zobowiązanie Ordynatora Oddziału i lekarzy do realizacji postanowień art. 36 ust. 1 ustawy w zakresie przechowywania bieżącej dokumentacji medycznej w pokoju lekarskim; obecnie dokumentacja medyczna przechowywana jest w zamykanych szafach i nie jest dostępna osobom nieupoważnionym,

2) w systemie informatycznym „B” jest rejestrowana data wprowadzenia danych, system jest obsługiwany przez jedną osobę i dane nie są udostępniane; system informatyczny „B” zapewnia sporządzenie i wydrukowanie raportu zawierającego informacje o dacie pierwszego wprowadzenia danych do tego systemu,

3) zainstalowanie programu antywirusowego na stacji roboczej systemu informatycznego „A”,

4) zainstalowanie programu antywirusowego zabezpieczającego system informatyczny o nazwie „C”,

5) zakupienie nowego sprzętu z systemem operacyjnym „G”, który zostanie podłączony do domeny i autentyfikacja będzie kontrolowana przez serwer; została wskazana jedna osoba upoważniona do obsługi systemu informatycznego „B”, tym samym nie ma konieczności rejestrowania dla tego użytkownika identyfikatora w systemie informatycznym „B”,

6) wprowadzenia do systemu informatycznego o nazwie „E” ośmioznakowego hasła zawierającego małe i wielkie litery oraz cyfry i opcjonalnie znaki specjalne.

Jednocześnie należy uwzględnić wyjaśnienia strony, z których wynika, że dane osobowe nie są przekazywane odbiorcom w rozumieniu art. 7 pkt 6 ustawy, tym samym brak zapewnienia przez systemy informatyczne o nazwach „B” i „A” odnotowania informacji o odbiorcach oraz zapewnienia wydrukowania raportu zawierającego te informacje, nie stanowi naruszenia § 7 ust. 4



i § 7 ust. 3 rozporządzenia. Ponadto, w związku z zaniechaniem użytkowania systemu informatycznego „D”, należy uznać, że postępowanie w zakresie uchybień dotyczących tego systemu stało się bezprzedmiotowe.

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.