



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 3 grudnia 2009 r.

DIS/DEC – 1207/44995/09

dot. DIS-K-421/130/09

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, art. 22 w związku z art. 36 ust. 1 i ust. 2, art. 37, art. 39 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.), § 4 i § 5 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 Regionalny Szpital Specjalistyczny im. (...) w (...), z siedzibą w (...),

I. Nakazuję Regionalnemu Szpitalowi Specjalistycznemu (...), przywrócenie stanu zgodnego z prawem w procesie przetwarzania danych osobowych, poprzez:

1. Zabezpieczenie dokumentacji zawierającej dane osobowe przechowywanej w pomieszczeniu nr 8, opisanym nazwą „Księgowość Zarządzająca” i pomieszczeniu opisanym nazwą „Druki”, przed jej udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem - w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna,

- 2. Opracowanie procedury określającej sposób zabezpieczenia pomieszczeń i sposób postępowania z kluczami do pomieszczeń oraz prowadzenie ewidencji wydawanych i zdawanych kluczy do pomieszczeń - w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna**
 - 3. Uzupełnienie polityki bezpieczeństwa, prowadzonej w formie dokumentu o nazwie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Regionalnym Szpitalu Specjalistycznym (...)\", o wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe - w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna;**
 - 4. Nadanie osobom zatrudnionym przy przetwarzaniu danych osobowych, upoważnień do przetwarzania danych osobowych – od dnia, w którym niniejsza decyzja stanie się ostateczna.**
 - 5. Prowadzenie w Regionalnym Szpitalu Specjalistycznym (...), ewidencji osób upoważnionych do przetwarzania danych osobowych - od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- II. W pozostałym zakresie postępowanie umarzam.**

U z a s a d n i e n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę (sygn. akt DIS-K-421/130/09) w Regionalnym Szpitalu Specjalistycznym (...), zwanym dalej także Szpitalem, 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. Nr 100, poz. 1024), zwanym dalej rozporządzeniem.

W toku kontroli odebrano od Dyrektora Szpitala oraz pracowników Szpitala 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 DIS-K-421/130/09), który został podpisany przez Dyrektora Szpitala.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Regionalny Szpital Specjalistyczny (...), jako administrator danych naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niezastosowaniu odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności niezabezpieczeniu danych przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną (art. 36 ust. 1 ustawy), gdyż jak ustalono w toku kontroli:

- w pomieszczeniu nr 8, opisanym nazwą „Księgowość Zarządzająca”, dokumentacja zawierająca dane osobowe pracowników przechowywana jest w segregatorach ułożonych na szafkach biurowych,
- w niezabezpieczonym (otwartym) pomieszczeniu opisanym nazwą „Druki”, w segregatorze opisanym - „Pacjenci z UE 2004 – 2005” przechowywana jest dokumentacja zawierająca dane osobowe pacjentów.

Ponadto, w toku kontroli ustalono, iż po zakończeniu dnia pracy klucze do pomieszczeń pozostawiane są w drzwiach, w celu umożliwienia dostępu do tych pomieszczeń osobom wykonującym prace porządkowe. W Szpitalu nie zostały opracowane procedury określające sposób zabezpieczenia pomieszczeń, jak również sposób postępowania z kluczami do pomieszczeń w których przetwarzane są dane osobowe. Ustalono również, iż w Szpitalu nie jest prowadzona ewidencja wydawanych i zdawanych kluczy do pomieszczeń.

2. Nieopracowaniu i niewdrożeniu do stosowania polityki bezpieczeństwa, o której mowa w § 4 rozporządzenia.

3. Nieopracowaniu i niewdrożeniu do stosowania instrukcji zarządzania systemem informatycznym, zawierającej informacje o których mowa w § 5 rozporządzenia.

4. Nienadaniu osobom zatrudnionym przy przetwarzaniu danych osobowych upoważnień do przetwarzania danych osobowych (art. 37 ustawy).

5. Nieprowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ust. 1 ustawy).

Pismem z dnia 22 października 2009 r. (sygn. DIS-K-421/130/09/38789), stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Szpital został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji o prawie do wypowiedzenia się co do zebranych dowodów i materiałów.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Szpitala, pismem z dnia 30 października 2009 r., (znak: SPZOZ-166/TAS/2009), przesłał wyjaśnienia w zakresie stwierdzonych uchybień oraz pozostałe dowody mające potwierdzić ich usunięcie.

Ze złożonych wyjaśnień wynika, iż:

1. Dyrektor Szpitala wydał w dniu 20 października 2009 r. polecenie służbowe w sprawie zabezpieczenia danych osobowych przed dostępem osób nieupoważnionych.
2. W trakcie opracowywania jest projekt procedury określającej sposób zabezpieczenia pomieszczeń, jak również określającej sposób postępowania z kluczami do pomieszczeń, w których przetwarzane są dane osobowe.
3. Dyrektor Szpitala Zarządzeniem Nr 52/2009 z dnia 18 września 2009 r. wdrożył do stosowania politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym.
4. Administrator bezpieczeństwa informacji złożył w dniu 29 października 2009 r. oświadczenie, z treści którego wynika, iż od dnia 10 sierpnia 2009 r. w Szpitalu prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.

Ponadto, do ww. pisma załączono dokumenty mające potwierdzić usunięcie uchybień stwierdzonych w toku kontroli, tj.

- kserokopię Zarządzenia nr 44/2009 z dnia 10 sierpnia 2009 r. Dyrektora Szpitala w sprawie wykonania obowiązków wynikających z art. 37, art 38, i art 39 ustawy o ochronie danych osobowych,
- kserokopię Zarządzenia nr 52/2009 z dnia 18 września 2009 r. Dyrektora Szpitala w sprawie wdrożenia polityki bezpieczeństwa, wraz z kserokopią załączników, stanowiących dokumenty o nazwach: „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Regionalnym Szpitalu Specjalistycznym im. Dr Wł. Biegańskiego w Grudziądzu” i „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Regionalnym Szpitalu Specjalistycznego(...)”,
- kserokopię polecenia służbowego Dyrektora Szpitala z dnia 20 października 2009 r.,
- kserokopię oświadczenia administratora bezpieczeństwa informacji z dnia 29 października 2009 r.

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, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

W toku kontroli ustalono, iż w pomieszczeniu nr 8 opisanym nazwą „Księgowość Zarządzająca”, dokumentacja w zapisie papierowym zawierająca dane osobowe przechowywana jest w segregatorach, ułożonych na szafkach biurowych. Ponadto, w toku kontroli stwierdzono,

iż w niezabezpieczonym (otwartym) pomieszczeniu opisanym nazwą „Druki”, przechowywany jest m. in. segregator opisany „Pacjenci z UE 2004 – 2005”, w którym przechowywane są dokumenty o nazwie „zestawienia pacjentów Unii Europejskiej za 2005 r. Szpital w (...)”. Zestawienia te zawierają imię i nazwisko pacjenta, nazwę oddziału szpitalnego, numer faktury i datę jej wystawienia, jak również kwotę należną za dane świadczenie medyczne. Do zestawień tych załączone są faktury wraz z kartą informacyjną leczenia szpitalnego. Karty informacyjne w swej treści zawierają: imię i nazwisko pacjenta, określenie rodzaju udzielonego świadczenia, przebieg choroby, zastosowane leczenie, jak również zalecenia lekarskie. Do pliku dokumentów, o których mowa powyżej, załączone są również kserokopie dokumentów sporządzonych w językach obcojęzycznych, potwierdzających ubezpieczenie danego pacjenta.

Dodatkowo ustalono, iż w Szpitalu nie zostały opracowane procedury określające sposób zabezpieczenia pomieszczeń, jak również sposób postępowania z kluczami do pomieszczeń w których przetwarzane są dane osobowe. Ponadto, jak ustalono w Szpitalu nie jest prowadzona ewidencja wydawanych i zdawanych kluczy do pomieszczeń. Pracownicy po zakończeniu dnia pracy klucze do pomieszczeń pozostawiają w drzwiach w celu umożliwienia dostępu do tych pomieszczeń osobom wykonującym prace porządkowe. Osoby sprzątające po wykonaniu prac porządkowych zamykają pomieszczenia, a klucze do tych pomieszczeń, w zamkniętym worku przekazują do dyspozytorki pogotowia ratunkowego zlokalizowanego w (...).

Pismem z dnia 30 października 2009 r., (znak: SPZOZ-166/TAS/2009) stanowiącymi odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Szpitala poinformował, iż w dniu 20 października 2009 r. wydał polecenie służbowe w sprawie zabezpieczenia danych osobowych przed dostępem osób nieupoważnionych. W piśmie tym poinformował również, iż w trakcie opracowywania jest projekt procedury określającej sposób zabezpieczenia pomieszczeń i regulującej sposób postępowania z kluczami do pomieszczeń, w których przetwarzane są dane osobowe. Dyrektor Szpitala nie przesłał jednak żadnych dowodów potwierdzających usunięcie przedmiotowych uchybień.

Wobec powyższego należy podkreślić, iż sam zamiar podjęcia działań w celu usunięcia uchybień jest zdarzeniem przyszłym i niepewnym, a tym samym nie stanowi podstawy do uznania, że został przywrócony stan zgodny z prawem w zakresie, o którym mowa powyżej.

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, zwana dalej „instrukcją”. Zgodnie z ust. 2, dokumentację, o której mowa

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

Zgodnie z § 4 pkt 1 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1 rozporządzenia, zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Jak ustalono w toku kontroli w Szpitalu nie została opracowana i wdrożona polityka bezpieczeństwa.

W piśmie z dnia 30 października 2009 r., (znak: SPZOZ-166/TAS/2009), Dyrektor Szpitala wyjaśnił, iż Zarządzeniem Nr 52/2009 z dnia 18 września 2009 r. wprowadził do stosowania dokument o nazwie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Regionalnym Szpitalu Specjalistycznym im. Dr Wł. Biegańskiego w Grudziądzu”. Ponadto, do ww. pisma załączona została kserokopia ww. dokumentu. Przesłany dokument nie zawiera jednak informacji, o których mowa w § 4 pkt 1 rozporządzenia, tj. nie zawiera wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Biorąc powyższe pod uwagę, Szpital jest zobowiązany do przywrócenia stanu zgodnego z prawem, w zakresie uzupełnienia polityki bezpieczeństwa prowadzonej w formie dokumentu o nazwie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Regionalnym Szpitalu Specjalistycznym (...)” o informacje, o których mowa powyżej.

Zgodnie z art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

W toku czynności kontrolnych ustalono, iż osoby dopuszczone do przetwarzania danych osobowych w Szpitalu nie posiadają upoważnień nadawanych przez administratora danych.

Pismem z dnia 30 października 2009 r., (znak: SPZOZ-166/TAS/2009) stanowiącymi odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Szpitala przesłał kserokopię Zarządzenia nr 44/2009 z dnia 10 sierpnia 2009 r. z treści którego wynika, iż Dyrektor Szpitala zobowiązuje administratora bezpieczeństwa informacji do przygotowania upoważnień administratora danych do przetwarzania danych osobowych. Z przesłanych wyjaśnień nie wynika jednak, czy Dyrektor Szpitala nadał upoważnienia do przetwarzania danych osobowych wszystkim osobom dopuszczonym do przetwarzania danych osobowych, jak również nie przesłano przykładowej kopii (wypełnionego) upoważnienia, która potwierdzałaby przywrócenie w tym zakresie stanu zgodnego z prawem.

Zgodnie z art. 39 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

- 1) imię i nazwisko osoby upoważnionej,
- 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

W toku czynności kontrolnych ustalono, że w Szpitalu nie jest prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych.

W piśmie z dnia 30 października 2009 r., (znak: SPZOZ-166/TAS/2009) Dyrektor Szpitala wyjaśnił, iż administrator bezpieczeństwa informacji złożył w dniu 29 października 2009 r. oświadczenie, z treści którego wynika, iż w Szpitalu prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.

W świetle powyższych ustaleń nie można uznać, iż uchybienie, o którym mowa powyżej zostało usunięte, gdyż Szpital nie przedstawił dowodu w postaci kserokopii przykładowych stron prowadzonej ewidencji osób upoważnionych do przetwarzania danych osobowych.

Jednocześnie na podstawie złożonych przez Szpital pisemnych wyjaśnień i przedstawionych dokumentów należy uznać, iż pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania zostały usunięte, tj.:

- opracowano i wdrożono dokument o nazwie „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Regionalnym Szpitalu Specjalistycznym (...)”, który zawiera informacje, o których mowa w § 5 rozporządzenia,
- opracowano i wdrożono dokument o nazwie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Regionalnym Szpitalu Specjalistycznym (...)”, który zawiera informacje, o których mowa w § 4 pkt 2, pkt 3, pkt 4 i pkt 5 rozporządzenia.

Z uwagi na to, iż w toku postępowania usunięte zostały ww. uchybienia, stanowiące przedmiot niniejszego postępowania, dlatego w tym zakresie należało postępowanie umorzyć.

Stosownie 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 z każdej przyczyny powodującej brak jednego z elementów materialno prawnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z 21 stycznia 1999 r. SA/Sz1029/97).

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.