GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 13 maja 2014 r.

DIS/DEC – 454/14/36247
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 2013 r., poz. 267), art. 12 pkt 2, art. 18 ust. 1 pkt 1, art. 22 w związku z art. 36 ust. 1, 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 § 7 ust. 1 pkt 2 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) oraz częścią A pkt II ust. 2 lit. a, lit. b, A pkt III ppkt 1, A pkt III ppkt 2, B pkt VIII załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez […] Szpital […] w K.,

I. Nakazuję […] Szpitalowi […] w K., jako administratorowi danych osobowych przywrócenie stanu zgodnego z prawem w procesie przetwarzania danych osobowych, poprzez:

1. Zapewnienie, aby w systemie informatycznym o nazwie „A" (system służący do przetwarzania danych osobowych pacjentów w związku z wykonywaniem badań […]) rejestrowany był dla każdego użytkownika odrębny identyfikator, a dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia – w terminie 60 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Zapewnienie, aby w systemie informatycznym o nazwie o nazwie „B” (system służący do przetwarzania danych osobowych w związku z prowadzoną rejestracją skierowań na badania i wyników badań) rejestrowany był dla każdego użytkownika odrębny identyfikator, a dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia - w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Zapewnienie, aby hasło używane do uwierzytelnienia użytkownika w systemie informatycznym o nazwie „B” składało się co najmniej z 8 znaków i zawierało wielkie litery – w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Zapewnienie, aby system informatyczny o nazwie „A” dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym, odnotowywał identyfikator użytkownika wprowadzającego dane do tego systemu – w terminie 60 dni 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 […]) w […] Szpitalu […] w K. (zwanym dalej „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”. Zakresem kontroli objęto zabezpieczenie danych osobowych pacjentów przetwarzanych przez […] Szpital […] w K.

W toku kontroli odebrano od 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, który został podpisany przez Dyrektora Szpitala.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych […] Szpital […] w K., jako administrator danych naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niezapewnieniu, aby w systemie informatycznym o nazwie „A” rejestrowany był dla każdego użytkownika odrębny identyfikator; dostęp do danych był możliwy wyłącznie po wprowadzeniu

identyfikatora i dokonaniu uwierzytelnienia (art. 36 ust. 1 ustawy w związku z częścią A pkt II ust. 2 lit. a, lit. b załącznika do rozporządzenia).

2. Niezapewnieniu, aby w systemie informatycznym o nazwie „B" rejestrowany był dla każdego użytkownika odrębny identyfikator, a dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia (art. 36 ust. 1 ustawy w związku z częścią A pkt II ust. 2 lit. a, lit. b załącznika do rozporządzenia).

3. Niezabezpieczeniu systemu informatycznego o nazwie „A" przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (art. 36 ust. 1 ustawy w związku z częścią A pkt III ppkt 1 załącznika do rozporządzenia).

4. Niezabezpieczeniu systemu informatycznego o nazwie „B" przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (art. 36 ust. 1 ustawy w związku z częścią A pkt III ppkt 2 załącznika do rozporządzenia).

5. Niezapewnieniu, aby hasło używane do uwierzytelnienia użytkownika w systemie informatycznym o nazwie „B" składało się co najmniej z 8 znaków i zawierało wielkie litery (art. 36 ust. 1 ustawy w związku z częścią B pkt VIII załącznika do rozporządzenia).

6. Niezapewnieniu przez administratora danych zgodnie z art. 38 ustawy, kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone, gdyż system informatyczny o nazwie „A" nie zapewnia odnotowania dla każdej osoby, której dane osobowe są przetwarzane w tym systemie, identyfikatora użytkownika wprowadzającego dane do tego systemu (§ 7 ust. 1 pkt 2 rozporządzenia).

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy. Pismem zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie (sygn. […]), administrator danych został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Szpitala pismem z dnia […] marca 2014 r. (znak: […]), przesłał wyjaśnienia w zakresie stwierdzonych uchybień. Ze złożonych wyjaśnień wynika, iż:

1. System informatyczny o nazwie „A" zostanie zastąpiony modułem o nazwie „C" - moduł systemu informatycznego o nazwie „D" (system informatyczny służący do przetwarzania danych osobowych pacjentów w związku z wykonywaniem badań oraz leczeniem pacjentów). Planowana data uruchomienia tego modułu przewidziana jest na koniec miesiąca maja 2014 r. Po zakończonym procesie wdrożenia przedmiotowego modułu pracownicy Szpitala zostaną odpowiednio przeszkoleni w zakresie jego użytkowania.

2. Na stanowisku komputerowym, na którym użytkowany jest system informatyczny o nazwie „A” zainstalowany został program antywirusowy o nazwie „E”.
3. Hasło używane do uwierzytelnienia użytkownika w systemie informatycznym o nazwie „B” składała się co najmniej z 8 znaków i zawiera wielkie litery.
4. System informatyczny o nazwie „B” został zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, gdyż komputer na którym użytkowany jest ww. system wyposażony został w zasilacz UPS.

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

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

1. Zgodnie z częścią A pkt II ust. 2 lit. a, lit. b załącznika do rozporządzenia, jeżeli dostęp dodanych przetwarzanych w systemie informatycznym posiadają, co najmniej dwie osoby, wówczas zapewnia się, aby:
a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,
b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

1.1. W toku kontroli ustalono, iż dostęp do systemu informatycznego o nazwie „A” (system służący do przetwarzania danych osobowych pacjentów w związku z wykonywaniem badań […]) możliwy jest po wprowadzeniu identyfikatora wspólnego dla wszystkich użytkowników ww. systemu, bez wprowadzania hasła.

W piśmie z dnia […] marca 2014 r. (znak: […]), stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Szpitala poinformował, iż system informatyczny o nazwie „A” zostanie zastąpiony modułem o nazwie „C” (moduł systemu informatycznego o nazwie „D”). Planowana data uruchomienia modułu o nazwie „C” przewidziana jest na koniec miesiąca maja 2014 r. Po zakończonym procesie wdrożenia przedmiotowego modułu pracownicy zostaną odpowiednio przeszkoleni w zakresie jego użytkowania.

Odnosząc się do ww. wyjaśnień, stwierdzić należy, iż nadal nie został przywrócony stan zgodny z prawem w zakresie, o którym mowa powyżej.

1.2. W toku kontroli ustalono, iż dostęp do systemu informatycznego o nazwie „B” (system służący do przetwarzania danych osobowych w związku z prowadzoną rejestracją skierowań

na badania i wyników badań) możliwy jest po wprowadzeniu indywidualnego hasła, bez wprowadzania indywidualnego identyfikatora.

W odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, Dyrektor Szpitala nie odniósł się do przedmiotowego uchybienia, w związku z powyższym należy uznać, iż nie został w tym zakresie przywrócony stan zgodny z prawem.

II. 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.

Zgodnie z § 7 ust. 1 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 identyfikatora użytkownika wprowadzającego dane do systemu.

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

W toku kontroli ustalono, iż system informatyczny o nazwie „A” nie zapewnia odnotowania identyfikatora użytkownika wprowadzającego dane do systemu.

W odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego Dyrektor Szpitala poinformował, iż system informatyczny o nazwie „A” zostanie zastąpiony modułem systemu informatycznego o nazwie „D” – tj. modułem o nazwie „C”, który spełnia wymogi dotyczące ochrony danych osobowych. Planowany termin uruchomienia tego modułu przewidziany jest na koniec miesiąca maja 2014 r.

Odnosząc się do ww. wyjaśnień, stwierdzić należy, iż nadal nie został przywrócony stan zgodny z prawem w zakresie, o którym mowa powyżej.

Jednocześnie na podstawie złożonych przez Dyrektora Szpitala wyjaśnień należy uznać, iż w toku postępowania usunięte zostały pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot niniejszego postępowania, poprzez:

1. Zabezpieczenie systemu informatycznego o nazwie „A” przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, gdyż na stanowisku komputerowym, na którym użytkowany jest ww. system informatyczny zainstalowany został program antywirusowy o nazwie „E” (art. 36 ust. 1 ustawy w związku z częścią A pkt III ppkt 1 załącznika do rozporządzenia).

2. Zabezpieczenie systemu informatycznego o nazwie „B” przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, gdyż komputer na którym użytkowany jest

ww. system informatyczny wyposażony został w zasilacz UPS (art. 36 ust. 1 ustawy w związku z częścią A pkt III ppkt 2 załącznika do rozporządzenia).

3. Obecnie hasło używane do uwierzytelnienia użytkownika w systemie informatycznym o nazwie „B" składa się co najmniej z 8 znaków i zawiera wielkie litery (art. 36 ust. 1 ustawy w związku z częścią B pkt VIII załącznika do rozporządzenia).

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe w całości albo w części, organ administracji publicznej wydaje decyzję o umorzeniu postępowania odpowiednio w całości albo w części. Przesłanką umorzenia postępowania, na podstawie art. 105 § 1 k.p.a. jest bezprzedmiotowość postępowania „z jakiejkolwiek przyczyny", czyli z 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. S.A./Sz1029/97).

Z uwagi na to, iż pozostałe uchybienia będące przedmiotem niniejszego postępowania administracyjnego zostały usunięte, postępowanie należało w tym zakresie umorzyć.

W świetle dokonanych ustaleń, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

W razie niewykonania decyzji w terminie, zostanie wobec podmiotu zobowiązanego do jej wykonania wszczęte postępowanie egzekucyjne na podstawie przepisów ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954, z późn. zm.).

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.