GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Edyta Bielak - Jomaa

Warszawa, dnia 24 lipca 2015 r.

DIS/DEC-616/15/66979
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, z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 oraz art. 22 w związku z art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, z późn. zm.), a także częścią A pkt II ust. 2 ppkt a, częścią A pkt IV ust. 2, częścią B pkt VIII oraz częścią C pkt XIII załącznika do 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 Samodzielny Publiczny Zakład Opieki Zdrowotnej pod nazwą Szpital Powiatowy w […] (dalej: Szpital),

I. Nakazuję Szpitalowi, usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. Zastosowanie środków organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mających na celu zabezpieczenie danych osobowych pacjentów pozyskiwanych przez lekarzy zatrudnionych w Szpitalu prowadzących wywiad lekarski w Izbie Przyjęć przed ich

udostępnieniem osobom nieupoważnionym, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Zapewnienie, aby w systemie informatycznym o nazwie „A” (w którym przetwarzane są dane osobowe pacjentów) rejestrowany był dla każdego użytkownika odrębny identyfikator, w terminie miesiąca dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Zapewnienie, aby zmiana hasła do systemu informatycznego o nazwie „A” następowała nie rzadziej niż co 30 dni, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Zapewnienie, aby zmiana hasła do systemu informatycznego o nazwie „B” (w którym przetwarzane są dane osobowe pacjentów) następowała nie rzadziej niż co 30 dni, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Zapewnienie, aby hasło do systemu informatycznego o nazwie „A” składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

6. Zapewnienie, aby hasło do systemu informatycznego o nazwie „B” składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

7. Zastosowanie środków kryptograficznej ochrony wobec danych osobowych pacjentów, wykorzystywanych do uwierzytelnienia w systemie informatycznym o nazwie „A”, które są przesyłane w sieci publicznej, w terminie 14 dni 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. […]) w Szpitalu 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 2014 r., poz. 1182, ze 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 toku kontroli odebrano od osób upoważnionych do reprezentacji 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 p.o. Dyrektora Szpitala.

Na podstawie materiału dowodowego zgromadzonego w toku kontroli ustalono, że w procesie przetwarzania danych osobowych Szpital, jako administrator danych, naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1) niezastosowaniu środków organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mających na celu zabezpieczenie danych osobowych pacjentów pozyskiwanych przez lekarzy zatrudnionych w Szpitalu prowadzących wywiad lekarski w Izbie Przyjęć przed ich udostępnieniem osobom nieupoważnionym (art. 36 ust. 1 ustawy),

2) nieopracowaniu pisemnych procedur dotyczących przekazywania do składnicy akt oraz wypożyczenia ze składnicy akt dokumentacji zawierającej dane osobowe pacjentów (art. 36 ust. 1 ustawy),

3) niezastosowaniu odpowiednich środków technicznych zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych przetwarzaniem w składnicy akt (art. 36 ust. 1 ustawy),

4) niezapewnieniu, aby w systemie informatycznym nazwie „A" rejestrowany był dla każdego użytkownika odrębny identyfikator (część A pkt II ust. 2 ppkt a załącznika do rozporządzenia),

5) niezapewnieniu, aby zmiana hasła do systemu informatycznego o nazwie „A" następowała nie rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia),

6) niezapewnieniu, aby zmiana hasła do systemu informatycznego o nazwie „B" następowała nie rzadziej niż co 30 (część A pkt IV ust. 2 załącznika do rozporządzenia),

7) niezapewnieniu, aby hasło do systemu informatycznego o nazwie „A" składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne (część B pkt VIII załącznika do rozporządzenia),

8) niezapewnieniu, aby hasło do systemu informatycznego o nazwie „B" składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne (część B pkt VIII załącznika do rozporządzenia),

9) niezastosowaniu środków kryptograficznej ochrony wobec danych osobowych pacjentów, wykorzystywanych do uwierzytelnienia w systemie informatycznym o nazwie „A", które są przesyłane w sieci publicznej (część C pkt XIII załącznika do rozporządzenia).

W piśmie z dnia […] czerwca 2015 r. (sygn. […]), stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Szpital 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 […] czerwca 2015 r. (znak: […]) złożył wyjaśnienia, w których poinformował, iż:

1) Szpital zgodnie z art. 36 ust. 1 ustawy, zastosował środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych przed dostępem osób nieuprawnionych, zniszczeniem lub utratą. Ponadto, wnioski wynikające z ustaleń kontroli dotyczą uchybień, które mają charakter incydentalny lub wynikają z niewiedzy osób składających ustne wyjaśnienia,

2) uchybienie zaistniałe w Izbie Przyjęć, znajdującej się na parterze Szpitala jest jednorazowym zdarzeniem; wywiad lekarski i badanie pacjenta są przeprowadzane w wydzielonym, oznakowanym gabinecie diagnostyczno-zabiegowym, a pomieszczenie za wydzieloną przeszkloną ladą służy jedynie do rejestracji pacjentów oraz prowadzenia dokumentacji. W czasie kontroli pomieszczenia służące do badania pacjenta były okazywane, więc niezrozumiałe jest dlaczego nie zostało to uwzględnione w zawiadomieniu o wszczęciu postępowania,

3) wprowadzono i wdrożono instrukcję przekazywania historii choroby - na każdym etapie. Obecnie osoba przyjmująca potwierdza fakt otrzymania konkretnych dokumentów z zaznaczeniem daty oraz osoby przekazującej (dowód: Zarządzenie Dyrektora Szpitala Powiatowego w [...] nr […] z dnia […] czerwca 2015 r. w sprawie: wprowadzenia Instrukcji Obiegu Dokumentacji Medycznej w Szpitalu Powiatowym w […], Zarządzenie Dyrektora Szpitala Powiatowego w […] nr […] z dnia […] czerwca 2015 r. w sprawie: wprowadzenia Instrukcji Archiwalnej w Szpitalu Powiatowym w […]),

4) zakupiono czujniki przeciwpożarowe oraz wskaźniki nadmiernej wilgotności oraz zamontowano je w pomieszczeniach aktualnej składnicy akt,

5) w przypadku systemu informatycznego o nazwie „A” konta użytkowników są aktualnie tworzone. Poinstruowano pracowników Szpitala o konieczności użytkowania własnych kont użytkowników oraz obowiązku stosowania się do obowiązującej polityki bezpieczeństwa,

6) połączenie z serwerem jest szyfrowane, przy czym nie jest to zależne od Szpitala, połączenie działa wykorzystując system VPN. System „B” jest zintegrowany z systemem „C” tzn. że obowiązują te same konta i zasady ich obsługi,

7) poziom ochrony danych osobowych będzie ulegał podnoszeniu wraz z poziomem wiedzy użytkowników. W celu osiągnięcia zadowalających postępów, Szpital organizuje cykliczne szkolenia, realizowane przez firmy zewnętrzne oraz własny personel.

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

Odnosząc się do wyjaśnień Dyrektora Szpitala, iż uchybienie zaistniałe w Izbie Przyjęć, było jednorazowym zdarzeniem należy wskazać, że w toku kontroli przyjęto ustne wyjaśnienia od Pani […], Koordynatora Izby Przyjęć (tj. osoby posiadającej stosowną wiedzę w tym przedmiocie), z których jednoznacznie wynika, że zdarzały się przypadki, iż w Izbie Przyjęć lekarze przeprowadzali wywiad lekarski z pacjentami. Wówczas pozostali pacjenci Szpitala oczekujący na przyjęcie do Szpitala mieli możliwość usłyszenia treści rozmowy lekarza z pacjentem w trakcie przeprowadzanego wywiadu lekarskiego. Ponadto w toku dokonywanych oględzin dokumentacji zawierającej dane osobowe pacjentów przechowywanej w Izbie Przyjęć miało miejsce przyjmowanie pacjenta na Oddział Chorób Wewnętrznych przez lekarza ww. oddziału, w trakcie którego był przeprowadzany wywiad lekarski. Pozostałe osoby oczekujące na przyjęcie do Szpitala oraz inspektorzy zatrudnieni w Biurze Generalnego Inspektora Ochrony Danych Osobowych przeprowadzający w Szpitalu czynności kontrolne mieli możliwość pozyskania (usłyszenia) informacji dotyczących stanu zdrowia pacjenta, z którym był przeprowadzany wywiad lekarski.

Wobec powyższego nie można zgodzić się z twierdzeniem Dyrektora Szpitala, iż uchybienie zaistniałe w Izbie Przyjęć, znajdującej się na parterze Szpitala było jednorazowym zdarzeniem.

Jednocześnie należy podkreślić, iż z ustaleń kontroli jednoznacznie wynika, że wywiad lekarski przeprowadzany był w Izbie Przyjęć a nie w pomieszczeniu służącym do badania pacjenta, na które powołuje się w swych wyjaśnieniach Dyrektor Szpitala.

Należy podnieść, iż podstawową zasadą odnoszącą się do obowiązków związanych z zabezpieczeniem danych osobowych jest zasada proporcjonalności, zgodnie z którą środki organizacyjne, jakie administrator zobowiązany jest zastosować, powinny zapewnić ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych (J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz, Kraków 2007 r., str. 603). Zastosowanie przez administratora skutecznych środków, ma celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Środki organizacyjne winny prowadzić do wyeliminowania szkodliwych zdarzeń, a gdy to możliwe ograniczyć ryzyko ich pojawienia się.

W omawianym przypadku Szpital nie zastosował środków organizacyjnych, o których mowa w art. 36. ust. 1 ustawy, z uwagi na fakt, iż wywiad lekarski był przeprowadzany przez lekarza zatrudnionego w Szpitalu w obecności osób trzecich, a konsekwencją tego było udostępnienie danych osobowych pacjentów Szpitala osobom nieupoważnionym. Ponadto należy podnieść, iż każdy lekarz na mocy art. 40 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza

i lekarza dentysty (Dz. U. z 2008 r. Nr 136, poz. 857, z późn. zm.) ma obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu.

Administrator danych zgodnie z art. 36 ust. 1 ustawy jest zobowiązany zatem zastosować odpowiednie środki organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych przetwarzaniem. Ponadto należy zauważyć, iż Generalny Inspektor Ochrony Danych Osobowych nie może wskazywać, w jaki konkretny sposób podmiot zobowiązany ma ten obowiązek wykonać. Wybór sposobu wykonania tego obowiązku został pozostawiony Szpitalowi. Wskazanie przez organ konkretnego sposobu dopełnienia obowiązku ograniczyłoby swobodę podmiotu w doborze tych środków.

Szpital ma zatem obowiązek podjęcia działania, które zapewni poufność danych osobowych pacjenta przetwarzanych w związku z przeprowadzanymi wywiadami lekarskimi, tak aby osoby postronne nie miały możliwości pozyskania (usłyszenia) informacji dotyczących jego stanu zdrowia.

Zgodnie z częścią A pkt II ust. 2 ppkt a załącznika do rozporządzenia, jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator.

W toku czynności kontrolnych ustalono, że wszyscy pracownicy mający dostęp do systemu informatycznego o nazwie „A” używają tego samego loginu i hasła.

W związku z powyższym należy uznać, że Spółka nie spełnia wymogów, o których mowa w części A pkt II ust. 2 ppkt a załącznika do rozporządzenia, tj. nie zapewnia aby w systemie informatycznego o nazwie „A” rejestrowany był dla każdego użytkownika odrębny identyfikator.

Zgodnie z częścią A pkt IV ust. 2 załącznika do rozporządzenia, w przypadku gdy do uwierzytelnienia użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni.

W toku czynności kontrolnych ustalono, że hasło do systemu informatycznego o nazwie „A” oraz do systemu informatycznego o nazwie „B” nie jest zmieniane.

Mając na uwadze powyższe należy uznać, iż Spółka nie spełnia wymogów, o których mowa w części A pkt IV ust. 2 załącznika do rozporządzenia, tj. zmiana hasła w ww. systemach informatycznych następuje rzadziej niż co 30 dni.

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

W toku czynności kontrolnych ustalono, że hasło do systemu informatycznego o nazwie „A” składa się z 3 znaków, natomiast hasło do systemu informatycznego o nazwie „B” składa się z 5 znaków i zawiera tylko cyfry.

W związku z powyższym należy uznać, że Spółka nie spełnia wymogów, o których mowa w części B pkt VIII załącznika do rozporządzenia, tj. nie zapewnia aby do uwierzytelnienia użytkowników używane były hasła składające się z co najmniej 8 znaków i zawierające małe i wielkie litery oraz cyfry lub znaki specjalne.

Zgodnie z częścią C pkt XIII załącznika do rozporządzenia, administrator stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

W toku czynności kontrolnych ustalono, że logowanie do systemu informatycznego o nazwie „A" jak i cały przesył informacji nie został zabezpieczony żadnymi metodami kryptograficznymi.

W związku z powyższym należy uznać, że Spółka nie zastosowała środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Odnosząc się do wyjaśnień Dyrektora Szpitala zawartych w piśmie z dnia […] czerwca 2015 r. w przedmiocie ww. uchybień, należy podnieść, iż nie przedstawiono dowodów potwierdzających, iż powyższe uchybienia zostały usunięte (np. w postaci wydruków z systemów informatycznych). Jednocześnie należy podnieść, iż samo podjęcie działań w celu usunięcia uchybienia dotyczącego zapewnienia, aby w systemie informatycznego o nazwie „[…]" rejestrowany był dla każdego użytkownika odrębny identyfikator nie stanowi podstawy do uznania, iż przywrócony został stan zgodny z prawem.

Jednocześnie, na podstawie przedstawionych wyjaśnień i innych dowodów w niniejszej sprawie, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.:

1) opracowano i wdrożono Instrukcję Archiwalną w Szpitalu Powiatowym w […] (dowód: Zarządzenie Dyrektora Szpitala Powiatowego w […] nr […] z dnia […] czerwca 2015 r. w sprawie: wprowadzenia Instrukcji Archiwalnej w Szpitalu Powiatowym w […]),

2) opracowano i wdrożono Instrukcję Obiegu Dokumentacji Medycznej w Szpitalu Powiatowym w […] (dowód: Zarządzenie Dyrektora Szpitala Powiatowego w […] nr […] z dnia […] czerwca 2015 r. w sprawie: wprowadzenia Instrukcji Obiegu Dokumentacji Medycznej w Szpitalu Powiatowym w […]),

3) zastosowano odpowiednie środki techniczne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych przetwarzaniem w składnicy akt, tj. zakupiono czujniki przeciwpożarowe i wskaźniki nadmiernej wilgotności oraz zamontowano je w pomieszczeniach składnicy akt.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Jak stwierdził Naczelny Sąd Administracyjny w uzasadnieniu wyroku z dnia 19 listopada 2001 r. (sygn. akt II SA 2702/00): „(...) skoro w toku prowadzonego (...) postępowania administracyjnego zniesiony został stan naruszenia prawa, którego miało dotyczyć rozstrzygnięcie, to postępowanie stało się bezprzedmiotowe".

W związku z tym, że w toku postępowania usunięte zostały pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, w tym zakresie należało je umorzyć.

Mając powyższe na uwadze, w tym stanie prawnym i faktycznym, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.

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.

Jednocześnie informuję, iż 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 2014 r. poz. 1619 z późn. zm.).