GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 5 marca 2012 r.

DIS/DEC -175/12/14285
dot. […]

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 ust. 1, art. 36 ust. 2, art. 38, art. 39 ust. 1 pkt 2-3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), § 4 pkt 2-4, § 7 ust. 1 pkt 1 – 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. Nr 100, poz. 1024) oraz częścią A pkt II, 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 Szpital Powiatowy w Z.,

nakazuję

Szpitalowi Powiatowemu w Z. (zwanemu dalej Szpitalem), jako administratorowi danych, usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

1. Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, poprzez:

1.1. Zapewnienie kontroli dostępu do archiwum mieszczącego się w piwnicy w budynku […] Szpitala oraz wyznaczenie osoby odpowiedzialnej za nadzór nad przechowywaną w nim dokumentacją i jej udostępnianiem, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

1.2. Opracowanie pisemnych procedur dotyczących: 1) prowadzenia archiwów/składnic akt Szpitala (w szczególności archiwum […]), postępowania z dokumentacją złożoną do archiwów/składnic akt, jej zabezpieczenia i udostępniania; 2) postępowania z kluczami od pomieszczeń Szpitala, w których przechowywane są dane osobowe; 3) zabezpieczenia dokumentacji papierowej zawierającej dane osobowe, w szczególności dane osobowe […], w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

1.3. Zainstalowanie systemu sygnalizacji pożaru w pomieszczeniach: archiwum mieszczącego się w piwnicy budynku […] Szpitala, składnicy akt […] […] kondygnacja budynku […]); składnicy podręcznej […] (pokój oznaczony „[…]"); oraz archiwum […] zlokalizowanego w budynku […] Szpitala na poziomie […], w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

1.4. Zabezpieczenie danych osobowych pacjentów Szpitala przechowywanych w dyżurkach […] w […] i […] Oddziale Chorób […] przed dostępem osób nieuprawnionych (pacjentów, osób odwiedzających itp.), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

1.5. Zabezpieczenie danych osobowych pacjentów Szpitala (historii chorób) przechowywanych w gabinecie […] w [..] Oddziale Chorób […] przed dostępem osób nieuprawnionych (pacjentów, salowych, itp.), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

1.6. Rejestrowanie w związku z udostępnianiem/wypożyczaniem historii chorób przekazanych do archiwum […] informacji umożliwiających ustalenie pracownika archiwum […], który udostępnił na miejscu lub wypożyczył poza archiwum ww. dokumentację (np. imię i nazwisko, podpis pracownika archiwum […], który udostępnia lub wypożycza poza archiwum historię choroby) oraz informacji pozwalających na ustalenie, czy dokumentacja ta została zwrócona do archiwum […], a jeżeli tak to kiedy i komu (np. imię i nazwisko, podpis pracownika archiwum […] odbierającego zwróconą historię choroby, datę zwrotu ww. dokumentacji), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Zapewnienie, aby przy dostępie do danych osobowych przetwarzanych w aplikacjach pakietu „A" (przetwarzanych na dyskach lokalnych stacji klienckich) były stosowane mechanizmy kontroli dostępu do danych osobowych, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Zapewnienie, aby w systemach informatycznych o nazwach: „B" (w którym przetwarzane są m.in. dane […]), „C" (w którym przetwarzane są dane […]) oraz „D" (w którym przetwarzane

są dane […]) dla każdego użytkownika był rejestrowany odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Zabezpieczenie systemów informatycznych o nazwach: „C" (w którym przetwarzane są dane […]), oraz „B" moduł K. i moduł P. (w którym przetwarzane są m.in. dane […]) przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Zapewnienie, aby hasło dostępu do serwerów systemów informatycznych o nazwach:„B" (system, w którym przetwarzane są m.in. dane […]) oraz „C" (system, w którym przetwarzane są dane […]) było zmieniane nie rzadziej niż co 30 dni, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

6. Zapewnienie, aby hasło używane do uwierzytelnienia użytkowników w systemie informatycznym o nazwie „D" (w którym przetwarzane są dane osobowe […]) składało się z co najmniej ośmiu znaków, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

7. Uzupełnienie opracowanej przez Szpital polityki bezpieczeństwa o następujące elementy: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

8. Zapewnienie, aby prowadzona w Szpitalu ewidencja osób upoważnionych do przetwarzania danych osobowych zawierała informacje o: dacie nadania i ustania oraz zakresie udzielonego im upoważnienia do przetwarzania danych osobowych, a w odniesieniu do osób, które przetwarzają dane osobowe w systemach informatycznych, także informacje o ich identyfikatorach w tych systemach, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

9. Zapewnienie, aby system informatyczny o nazwie „B" (w którym przetwarzane są m.in. dane […]) oraz system informatyczny o nazwie „C" (w którym przetwarzane są dane […]) dla każdej osoby, której dane osobowe są przetwarzane w tych systemach odnotowywały informacje o: dacie pierwszego wprowadzenia danych do systemu; identyfikatorze użytkownika wprowadzającego dane osobowe do systemu; źródle danych, w przypadku zbierania danych, nie od osoby, której one dotyczą; odbiorcach danych, którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

10. Zapewnienie, aby system informatyczny o nazwie „B" (w którym przetwarzane są m.in. dane […]) oraz system informatyczny o nazwie „C" (w którym przetwarzane są dane […]) dla każdej

osoby, której dane osobowe są przetwarzane w tych systemach odnotowywały informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

11. Zapewnienie, aby system informatyczny o nazwie „B" (w którym przetwarzane są m.in. dane […]) oraz system informatyczny o nazwie „C" (w którym przetwarzane są dane […]), dla każdej osoby, której dane osobowe są przetwarzane w tych systemach umożliwiały sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o: dacie pierwszego wprowadzenia danych do systemu; identyfikatorze użytkownika wprowadzającego dane osobowe do systemu; źródle danych, w przypadku zbierania danych, nie od osoby, której one dotyczą; odbiorcach danych, którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w Szpitalu Powiatowym w Z. (zwanym dalej również Szpitalem), w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. akt […]), 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 m.in. odebrano od pracowników 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. kontroli […]), który został podpisany przez Dyrektora Szpitala. Na podstawie całokształtu materiału dowodowego zgromadzonego w sprawie ustalono, że Szpital Powiatowy w Z., jako administrator danych, naruszył przepisy o ochronie danych osobowych. Stwierdzone uchybienia polegały na:

1. Niezastosowaniu 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,

zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy), z uwagi na:

1.1. Niezapewnienie kontroli dostępu do archiwum mieszczącego się w piwnicy w budynku […] Szpitala oraz niewyznaczenie osoby odpowiedzialnej za nadzór nad przechowywaną w nim dokumentacją, w szczególności w zakresie dotyczącym jej udostępniania osobom upoważnionym.

1.2. Nieopracowanie pisemnych procedur dotyczących: 1) prowadzenia archiwów/składnic akt Szpitala (w szczególności archiwum […]), postępowania z dokumentacją złożoną do archiwów/składnic akt, jej zabezpieczenia i wypożyczania; 2) postępowania z kluczami od pomieszczeń Szpitala, w których przechowywane są dane osobowe; 3) zabezpieczenia dokumentacji papierowej zawierającej dane osobowe, w szczególności dane osobowe […] Szpitala.

1.3. Niezainstalowanie systemu sygnalizacji pożaru w pomieszczeniach: archiwum mieszczącego się w piwnicy budynku […] Szpitala, składnicy akt […], ([…] kondygnacja budynku […]); składnicy podręcznej […] (pokój oznaczony […]); archiwum […] zlokalizowanych w budynku […] Szpitala na poziomie […].

1.4. Niezabezpieczenie danych osobowych pacjentów Szpitala przechowywanych w dyżurkach […] w […] i […] Oddziale Chorób […] przed dostępem osób nieuprawnionych (pacjentów, osób odwiedzających itp.).

1.5. Niezabezpieczenie danych osobowych pacjentów Szpitala (historii chorób) przechowywanych w gabinecie […] w […] Oddziale Chorób […] przed dostępem osób nieuprawnionych (pacjentów, salowych, itp.).

1.6. Nierejestrowanie, w związku z udostępnianiem/wypożyczaniem historii chorób przekazanych do archiwum […], informacji umożliwiających ustalenie pracownika archiwum […], który udostępnił na miejscu lub wypożyczył poza archiwum ww. dokumentację (np. imię i nazwisko, podpis pracownika archiwum […], który udostępnia lub wypożycza poza archiwum historię choroby) oraz informacji pozwalających na ustalenie, czy dokumentacja ta została zwrócona do archiwum […], a jeżeli tak to kiedy i komu (np. imię i nazwisko, podpis pracownika archiwum […] odbierającego zwróconą historię choroby, datę zwrotu ww. dokumentacji).

2. Niezapewnieniu, aby przy dostępie do danych osobowych przetwarzanych w aplikacjach pakietu „A” (przetwarzanych na dyskach lokalnych stacji klienckich) były stosowane mechanizmy kontroli dostępu do danych osobowych (część A pkt II ust. 1 załącznika do rozporządzenia).

3. Niezapewnieniu, aby w systemach informatycznych o nazwach: „B” (w którym przetwarzane są m.in. dane […]), „C” (w którym przetwarzane są dane […]) oraz „D” (w którym przetwarzane są dane osobowe […]) rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia (część A pkt II ust. 2 załącznika do rozporządzenia).

4. Niezabezpieczeniu systemów informatycznych o nazwach: „C” (w którym przetwarzane są dane […]), oraz „B” moduł K. i moduł P. (w którym przetwarzane są m.in. dane […]) przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (część A pkt III ppkt 1 załącznika do rozporządzenia).

5. Niezapewnieniu, aby hasło dostępu do serwerów systemów informatycznych o nazwach:„B” (system, w którym przetwarzane są m.in. dane […]) oraz „C” (system, w którym przetwarzane są dane […]) było zmieniane nie rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).

6. Niezapewnieniu, aby hasło używane do uwierzytelnienia użytkowników w systemie informatycznym o nazwie „D” (w którym przetwarzane są dane osobowe […] Szpitala) składało się z co najmniej ośmiu znaków (część B pkt VIII załącznika do rozporządzenia).

7. Niezawarciu w opracowanej przez Szpital polityce bezpieczeństwa elementów takich jak: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi (§ 4 pkt 2-4 rozporządzenia).

8. Niezapewnieniu, aby prowadzona w Szpitalu ewidencja osób upoważnionych do przetwarzania danych osobowych zawierała informacje o: dacie nadania i ustania oraz zakresie udzielonego upoważnienia do przetwarzania danych osobowych, a w odniesieniu do osób, które przetwarzają dane osobowe w systemach informatycznych, także informacje o ich identyfikatorach w tych systemach (art. 39 ust. 1 pkt 2 i 3 ustawy).

9. Niezapewnieniu, aby system informatyczny o nazwie „B” (w którym przetwarzane są m.in. dane […]) oraz system informatyczny o nazwie „C” (w którym przetwarzane są dane […]) dla każdej osoby, której dane osobowe są przetwarzane w tych systemach odnotowywały informacje o: dacie pierwszego wprowadzenia danych do systemu; identyfikatorze użytkownika wprowadzającego dane osobowe do systemu; źródle danych, w przypadku zbierania danych, nie od osoby, której one dotyczą; informacji o odbiorcach danych, którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia (§ 7 ust. 1 pkt 1 – 4 rozporządzenia).

10. Niezapewnieniu, aby system informatyczny o nazwie „B” (w którym przetwarzane są m.in. dane […]) oraz system informatyczny o nazwie „C” (w którym przetwarzane są dane […]) dla każdej osoby, której dane osobowe są przetwarzane w tych systemach odnotowywały informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych (§ 7 ust. 2 rozporządzenia).

11. Niezapewnieniu, aby system informatyczny o nazwie „B” (w którym przetwarzane są m.in. dane […]) oraz system informatyczny o nazwie „C” (w którym przetwarzane są dane […]) umożliwiały dla

każdej osoby, której dane osobowe są przetwarzane w tych systemach informatycznych sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o: dacie pierwszego wprowadzenia danych do systemu; identyfikatorze użytkownika wprowadzającego dane osobowe do systemu; źródle danych, w przypadku zbierania danych, nie od osoby, której one dotyczą; informacji o odbiorcach danych, którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia (§ 7 ust. 3 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 (nr […]), 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. Administrator danych nie skorzystał z ww. uprawnienia.

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

1. 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.

Jak ustalono w toku kontroli, w budynku […] Szpitala w piwnicy znajduje się pomieszczenie archiwum, w którym na odkrytych metalowych regałach przechowywane są dokumenty zawierające dane osobowe m.in.: listy płac, dokumenty dotyczące zasiłków chorobowych; dowody księgowe (faktury); akta osobowe pracowników; dowody do list płac i wykazy pełnionych dyżurów. W Szpitalu nie ma wyznaczonej jednej osoby odpowiedzialnej za ww. archiwum. Jest to archiwum wspólne dla Działu […] i Działu […], w tym […]. Pracownicy tych działów w razie potrzeby biorą klucze ze skrzynki metalowej znajdującej się w pokoju nr […] w celu skorzystania z materiałów znajdujących się w ww. archiwum. Z uwagi na powyższe ustalenia należy uznać, że Szpital nie zastosował w opisywanej sytuacji odpowiednich środków organizacyjnych w celu zapewnienia ochrony danych osobowych pracowników Szpitala zawartych w dokumentacji przechowywanej w archiwum Działu […] i Działu […], w tym […], gdyż nie wyznaczył osoby odpowiedzialnej za opisane powyżej archiwum, do której obowiązków należałoby w szczególności przyjmowanie i udostępnianie/wypożyczanie przechowywanej w nim dokumentacji, oraz umożliwił dostęp do kluczy od ww. archiwum szerokiemu kręgowi pracowników Szpitala.

Ponadto Dyrektor Szpitala zeznał w toku kontroli, iż w Szpitalu nie zostały opracowane pisemne procedury dotyczące: zabezpieczenia dokumentacji papierowej zawierającej dane osobowe, w szczególności odnoszące się do sposobu jej przechowywania i udostępniania; postępowania z kluczami do pomieszczeń w których odbywa się przetwarzanie danych osobowych; postępowania z dokumentacją archiwalną i jej zabezpieczenia. Z wyjaśnień Kierownika […], wynika natomiast, iż w Szpitalu nie zostały opracowane i wdrożone pisemne procedury dotyczące funkcjonowania archiwum […], które określałyby w szczególności sposób przyjmowania dokumentów do archiwum […] i ich udostępniania. W Rozdziale 12 „Instrukcji Kancelaryjnej" (§ 37 i § 38) wprowadzonej Zarządzeniem nr […] Dyrektora Szpitala Powiatowego w Z. z dnia […] kwietnia 2010 r. wskazano jedynie kilka elementów związanych z przygotowaniem dokumentacji do przekazania do archiwum. Z uwagi na powyższe uznać należy, że Szpital nie dopełnił obowiązku zastosowania odpowiednich środków organizacyjnych w celu zabezpieczenia danych osobowych przetwarzanych w Szpitalu w postaci papierowej przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem z uwagi na nieopracowanie pisemnych procedur, które regulowałyby kwestie dotyczace: 1) prowadzenia archiwów/składnic akt Szpitala (w szczególności archiwum […]), postępowania z dokumentacją złożoną do archiwów/składnic akt, jej zabezpieczenia i wypożyczania; 2) postępowania z kluczami od pomieszczeń Szpitala, w których przechowywane są dane osobowe; 3) zabezpieczenia dokumentacji papierowej zawierającej dane osobowe, w szczególności dane osobowe pacjentów Szpitala.

W tym miejscu należy jednak wskazać, iż w toku kontroli stwierdzono, iż fakt udostępnienia historii chorób z archiwum […] odnotowywany jest w dedykowanym do tego celu zeszycie. Wpisywane są w nim takie informacje jak: data udostępnienia/wypożyczenia oraz imię i nazwisko osoby, która pobrała historię choroby. Kiedy historia choroby pacjenta zostaje zwrócona ww. informacje są przekreślane w zeszycie. Niemniej jednak opisana powyżej praktyka nie jest wystarczająca, aby na jej podstawie możliwe było uznanie, iż Szpital zastosował wobec dokumentacji przechowywanej w archiwum […] odpowiednie środki organizacyjne w celu zabezpieczenia danych osobowych zawartych w tej dokumentacji przed ich udostępnieniem osobom nieupoważnionym oraz/lub utratą. W opisywanym zeszycie nie są bowiem rejestrowanie informacje umożliwiające ustalenie pracownika archiwum […], który udostępnił na miejscu lub wypożyczył poza obszar archiwum przechowywaną w nim dokumentację (np. imię i nazwisko, podpis pracownika archiwum […], który udostępnia lub wypożycza poza archiwum historię choroby) oraz informacje pozwalające na ustalenie, czy dokumentacja ta została zwrócona do archiwum […], a jeżeli tak to kiedy i komu (np. imię i nazwisko, podpis pracownika archiwum […] odbierającego zwróconą historię choroby, datę zwrotu ww. dokumentacji).

Ponadto w toku oględzin przeprowadzonych w budynku […] Szpitala w piwnicy, w której znajduje się pomieszczenie archiwum ustalono, iż w archiwum tym nie zainstalowano czujek przeciwpożarowych. Także na […] kondygnacji budynku […], gdzie znajduje się składnica akt […] (wejście z korytarza do części administracyjnej budynku […]) nie ma czujek przeciwpożarowych. Brak czujek przeciwpożarowych stwierdzono także w budynku […] Szpitala w pomieszczeniu, w którym znajduje się składnica podręczna […] (pawilon […], parter, pokój oznaczony […]) oraz w piwnicach (poziom […]), gdzie zlokalizowane są pomieszczenia archiwum […] Szpitala (dokonano oględzin trzech z sześciu pomieszczeń ww. archiwum […]). Szpital nie dopełnił zatem obowiązku odpowiedniego zabezpieczenia danych osobowych pacjentów i pracowników Szpitala przed ich uszkodzeniem lub zniszczeniem.

W toku czynności kontrolnych przeprowadzonych w Szpitalu dokonano także oględzin dyżurki […] w […] Oddziale Chorób […]. W ich wyniku ustalono, iż jest to wnęka sąsiadująca z korytarzem (brak drzwi, brak lady wydzielającej to pomieszczenie od korytarza z pacjentami). W ww. dyżurce […] stoją m.in. dwa biurka z szufladami bez zamków. W szufladach tych przechowywane są karty zleceń lekarskich i karty indywidualne pielęgnacyjne pacjentów. Oględzinom poddano również dyżurkę […] w […] Oddziale Chorób […]. Na ich podstawie stwierdzono, iż przed wejściem do opisywanej dyżurki […] znajduje się lada ze stanowiskiem pracy, która jednakże nie uniemożliwia osobom postronnym dostępu do przestrzeni służbowej dyżurki. Na ladzie tej (od strony stanowiska pracy) przechowywane są karty indywidualne pielęgnacyjne pacjentów. Należy jednocześnie zauważyć, iż w toku oględzin stwierdzono, iż po korytarzach […] i […] Oddziału […] odbywa się wzmożony ruch pacjentów tych oddziałów. Zatem zasadnym jest twierdzenie, iż w odniesieniu do danych osobowych znajdujących się w treści dokumentacji przechowywanej w ww. dyżurkach […] Szpital nie stosuje odpowiednich środków technicznych i organizacyjnych w celu ich zabezpieczenia przed dostępem osób nieuprawnionych (pacjentów, osób odwiedzających itp.).

Ponadto ustalono, iż historie choroby pacjentów […] Oddziału Chorób […] przechowywane są w […] na otwartym regale, gdyż lekarz dyżurny musi mieć łatwy i szybki dostęp do dokumentacji pacjentów przebywających na Oddziale. Jak wyjaśnił Ordynator […] Oddziału Chorób […], Lekarz wychodząc z […] zamyka go na klucz, który pozostawia w drzwiach lub jeżeli będzie przez dłuższy czas nieobecny pozostawia go w pokoju […]. Jednocześnie ustalono, iż […] Oddział Chorób […] pracuje całodobowo i odwiedzający mają wstęp na teren tego Oddziału Szpitala również całą dobę. Sprzątaniem gabinetu […] zajmują się salowe. Sprzątanie gabinetu […] odbywa się również bez obecności lekarzy. Tym samym, mając na względzie powyższe ustalenia, należy uznać, iż Szpital nie dopełnił obowiązku odpowiedniego zabezpieczenia danych osobowych pacjentów Szpitala (historii chorób) przechowywanych w gabinecie […] w […] Oddziale Chorób […] poprzez nie zabezpieczenie ww. dokumentów przed dostępem do nich osób nieuprawnionych (pacjentów, salowych, itp.).

2. Zgodnie z częścią A pkt II ust. 1 załącznika do rozporządzenia w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.

W toku czynności kontrolnych ustalono, że przy dostępie do danych osobowych przetwarzanych w aplikacjach pakietu „A" (przetwarzanych na dyskach lokalnych stacji klienckich) nie są stosowane mechanizmy kontroli dostępu do danych osobowych.

3. Zgodnie z częścią A pkt II ust. 2 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 oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

W toku kontroli ustalono, że w systemach informatycznych o nazwach: „B" (w którym przetwarzane są m.in. […]), „C" (w którym przetwarzane są dane […]) oraz „D" (w którym przetwarzane są dane […]) nie zapewnia się, aby dla każdego użytkownika systemu rejestrowany był odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

4. Zgodnie z częścią A pkt III ppkt 1 załącznika do rozporządzenia system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

W toku czynności kontrolnych ustalono, że systemy informatyczne służące do przetwarzania danych osobowych o nazwach: „B" (w którym przetwarzane są m.in. dane […]) oraz „B" moduł K. i moduł P. (w którym przetwarzane są dane […]) nie są zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

5. Zgodnie z częścią A pkt IV ust. 2 załącznika do rozporządzenia, w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.

W toku czynności kontrolnych ustalono, że hasło dostępu do serwerów systemów informatycznych o nazwach: „B" (w którym przetwarzane są m.in. dane […]), „C" (w którym przetwarzane są dane […]) jest zmieniane rzadziej niż co 30 dni.

6. 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 hasło używane do uwierzytelnienia użytkowników w systemie informatycznym o nazwie „D" (w którym przetwarzane są dane osobowe […]) składa się z siedmiu znaków.

7. Zgodnie z art 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. Jak stanowi § 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". Natomiast zgodnie z § 4 pkt 2-4 rozporządzenia polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami.

W toku kontroli ustalono, że opracowana w Szpitalu polityka bezpieczeństwa nie zawiera elementów takich jak: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami.

8. Zgodnie z art. 39 ust. 1 pkt 2 i 3 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

W toku czynności kontrolnych ustalono, że w Szpitalu jest prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych, jednak nie spełnia ona wymogów określonych w art. 39 ust. 1 pkt 2 i 3 ustawy, gdyż nie zawiera: daty nadania i ustania oraz zakresu upoważnienia do przetwarzania danych osobowych oraz identyfikatorów użytkowników, którzy przetwarzają dane osobowe w systemach informatycznych Szpitala.

9. 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 jak stanowi § 7 ust. 1 pkt 1 - 4 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; 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.

W toku czynności kontrolnych ustalono, że systemy informatyczne o nazwach: „B” (w którym przetwarzane są m.in. dane […]) oraz „C” (w którym przetwarzane są dane […]) nie zapewniają odnotowania informacji, o których mowa w § 7 ust. 1 pkt 1 - 4 rozporządzenia.

10. 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.

W toku czynności kontrolnych ustalono, że systemy informatyczne o nazwach: „B” oraz „C” nie zapewniają dla każdej osoby, której dane osobowe są przetwarzane w tych systemach odnotowania informacji, o których mowa w § 7 ust. 1 pkt 1 i 2 rozporządzenia (tj. daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu) automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

11. 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 ust. 1 rozporządzenia.

W toku czynności kontrolnych ustalono, że systemy informatyczne o nazwach: „B” oraz „C” nie zapewniają dla każdej osoby, której dane osobowe są przetwarzane w tych systemach informatycznych sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 pkt 1-4 rozporządzenia.

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.