GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
Ewa Kulesza

Warszawa, dnia 21 września 2001 r.

GI/DEC-DIS-118/01/812

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 (tekst jednolity: Dz. U. z 2000 r. Nr 98, póz. 1071), art. 18 ust. l pkt 1 w związku art. 39 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm), oraz § 14 ust. 3 i 6, § 16 pkt 3 i 4, § 17 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez […]Kasę Chorych […].

I. Nakazuję […]Kasie Chorych […]. usunięcie uchybień w procesie przetwarzania danych osobowych, w terminie trzech miesięcy od dnia, kiedy niniejsza decyzja stanie się ostateczna, poprzez:

1. Zapewnienie, aby dla każdej osoby, której dane są przetwarzane w systemach informatycznych: „A", „B" „C", „D", „E" oraz „F", systemy te odnotowywały informacje komu, kiedy i w jakim zakresie dane zostały udostępnione innym podmiotom.
2. Zapewnienie, aby systemy informatyczne: „A", „B" „C", „D", „E" oraz „F", służące do przetwarzania danych osobowych, umożliwiały udostępnienie na piśmie, w powszechnie

ul. Stawki 2
00-193 Warszawa
tel. (22)5310313
fax (22)5310301
www.giodo.gov.pl

zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, wraz z informacją komu, kiedy i w jakim zakresie dane zostały udostępnione innym podmiotom.

II. W pozostałym zakresie postępowanie umarzam.

Uzasadnienie

W dniach […] lutego 2001 r. upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych inspektorzy, na podstawie art. 14 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), zwanej dalej ustawą, przeprowadzili w […]Kasie Chorych […] zwanej dalej również „[…]KCh" lub „Kasą Chorych", kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. z powołaną wyżej ustawą i rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. (Dz. U. Nr 80, poz. 521 z późn. zm.), zwanym dalej rozporządzeniem. W trakcie kontroli odebrano od pracowników […]KCh ustne wyjaśnienia, skontrolowano system informatyczny służący do przetwarzania danych osobowych oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny szczegółowo opisany został w protokole kontroli, który został podpisany przez Dyrektora […]Kasy Chorych.

Na podstawie tak zgromadzonego w trakcie kontroli materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych […]Kasa Chorych, jako administrator danych naruszyła przepisy o ochronie danych osobowych. Stwierdzono m.in. następujące uchybienia:
1. Jeden identyfikator i odpowiadające mu hasło dostępu do aplikacji „G" używany był przez dwóch użytkowników.

2. W przypadku jednego użytkownika systemu kadrowo - płacowego hasło dostępu do aplikacji „F" nie było zmieniane.
3. Funkcjonująca w […]KCh ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych, nie obejmowała wszystkich osób zatrudnionych przy przetwarzaniu danych w zbiorze o nazwie „R". Ponadto, nie spełniała ona wymogów § 6 ust. 5 obowiązującej w […]KCh „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", zgodnie z którym administrator bezpieczeństwa informacji prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych zawierającą imię i nazwisko, identyfikator, komórkę organizacyjną oraz datę rejestracji i wyrejestrowania użytkownika.
4. System informatyczny „D" nie zapewniał odnotowania identyfikatora użytkownika wprowadzającego dane. Systemy informatyczne: „A", „B" „C", „D", „E" oraz „F", nie umożliwiały

odnotowania informacji komu, kiedy i w jakim zakresie dane zostały udostępnione innym podmiotom.
5. Systemy informatyczne: „A”, „B”, „C”, „D”, „E” oraz „F”, służące do przetwarzania danych osobowych, nie umożliwiały udostępnienia na piśmie, w powszechnie zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane wraz z informacją komu, kiedy i w jakim zakresie dane zostały udostępnione innym podmiotom.

Pismem z dnia […] lipca 2001 r., nr […], Generalny Inspektor Ochrony Danych Osobowych zwrócił się do administratora danych o złożenie wyjaśnień m.in. w zakresie ww. uchybień, a następnie w dniu […] sierpnia 2001 r. (pismo nr […]) wszczął z urzędu postępowanie administracyjne w przedmiocie wskazanych nieprawidłowości w celu wyjaśnienia okoliczności niniejszej sprawy.

W odpowiedzi na ww. pismo z dnia […] lipca 2001 r. oraz na zawiadomienie o wszczęciu postępowania administracyjnego Dyrektor […]Kasy Chorych pismami z dnia […] sierpnia 2001 r. (znak […]), […] sierpnia 2001 r. (znak […]) oraz […] września 2001 r. (znak […]) złożył wyjaśnienia, ustosunkowując się m.in. do ww. zarzutów.

Odnośnie uchybień wymienionych w pkt 1 i 2 zawiadomienia o wszczęciu postępowania administracyjnego poinformowano, że uchybienia te zostały usunięte po zakończeniu czynności kontrolnych przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych.

W nawiązaniu do uchybienia dotyczącego obowiązku określonego w art. 39 ust. 1 ustawy w piśmie z dnia […] sierpnia 2001 r. wyjaśniono, że tworzona jest ewidencja użytkowników systemu „C”. Jednocześnie wskazano, że ewidencja ta może być traktowana wyłącznie jako dodatkowe zabezpieczenie, wykraczające poza wymogi przewidziane przepisami o ochronie danych osobowych. Zdaniem […]KCh, administrator danych zobligowany jest jedynie do prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych u administratora. Ponadto, w piśmie z dnia […] sierpnia 2001 r. […]KCh wskazała, że powyższy obowiązek nie dotyczy użytkowników zewnętrznych systemu (w systemie „C” jest to personel świadczeniodawcy).

W piśmie z dnia […] września 2001 r. […]KCh poinformowała, że wdrożono mechanizm tworzenia raportu o każdym użytkowniku systemu i nadanych mu uprawnieniach. Obecnie odnotowuje się następujące informacje o każdym użytkowniku systemu: imię nazwisko, identyfikator użytkownika, a także datę jego wprowadzenia oraz usunięcia. Na potwierdzenie powyższych wyjaśnień załączono przykładowy raport o użytkowniku systemu. Ponadto poinformowano, że odrębnie prowadzony jest wykaz obejmujący wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych.

W nawiązaniu do uchybień polegających na niedopełnieniu obowiązków określonych w § 16 i 17 rozporządzenia w piśmie z dnia […] sierpnia 2001 r. […]KCh zarzuciła, że w pismach z dnia […] lipca 2001 r. i […] sierpnia 2001 r. Generalny Inspektor nie określił jakich elementów systemu informatycznego dotyczą uchybienia. Podniesiono, że pojęcie systemu informatycznego zostało zdefiniowane w § 1 pkt 1 rozporządzenia jako „system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje". Zdaniem Kasy Chorych definicja ta nie ogranicza systemu informatycznego wyłącznie do sprzętu i oprogramowania, ale obejmuje również element organizacyjny związany z przetwarzaniem danych osobowych („ludzie"). Z tego punktu widzenia obowiązek zapewnienia, aby system informatyczny odnotował określone informacje, a następnie udostępniał je w formie pisemnej nie musi oznaczać wymogu wprowadzenia w odniesieniu do struktur baz danych i aplikacji nimi zarządzających odpowiednich opcji rejestrujących oraz umożliwiających wydrukowanie danych. Dla wykonania obowiązku można bowiem wykorzystać ludzi, jako element systemu informatycznego. Przykładowo mogą oni odnotowywać przewidziane prawem informacje w odrębnych, niekoniecznie zintegrowanych rejestrach (w tym również w sposób tradycyjny), a następnie (w razie potrzeby) zestawiać dane w zbiorczą informację w ten sposób, aby mogła być udostępniana na piśmie w powszechnie zrozumiałej formie. Zdaniem […]KCh wystarczy więc wprowadzenie przez administratora danych zasad organizacyjnych gwarantujących odpowiednie postępowanie personelu obsługującego system.

Niezależnie od prezentowanego w tym zakresie stanowiska pismem z dnia […] września 2001 r, […]KCh oświadczyła, że wprowadzono automatyczne odnotowanie identyfikatora użytkownika wprowadzającego dane osobowe do systemu „D". Ponadto poinformowano, że administrator danych jest w trakcie realizacji warunków określonych w pkt 4 i 5 zawiadomienia o wszczęciu postępowania administracyjnego. Jednakże ze względu na złożoność systemu informatycznego eksploatowanego w […]KCh oraz przebudowę znaczącej jego części […], oświadczono, że w terminie 3 miesięcy wprowadzone zostaną funkcje zapewniające odnotowanie udostępnień danych osobowych, zintegrowane ze wszystkimi zbiorami wskazanymi w pkt 4 zawiadomienia o wszczęciu postępowania administracyjnego (za wyjątkiem systemu „B"). Do dnia […] grudnia 2001 r. wdrożona zostanie opcja zapewniająca odnotowywanie informacji wskazanych w pkt 5 ww. zawiadomienia. Ponadto poinformowano, że w związku z całkowitą przebudową „B" oraz zmianą platformy sprzętowej nie nastąpi modyfikacja dotychczas eksploatowanego systemu. Nowa wersja tego systemu spełniająca wymogi określone w § 16 i 17 rozporządzenia zostanie przygotowana do dnia […] stycznia 2002 r.

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

Zgodnie z § 16 rozporządzenia, dla każdej osoby, której dane są przetwarzane w systemie informatycznym, system ten powinien zapewniać odnotowanie: daty pierwszego wprowadzenia danych tej osoby, źródła pochodzenia danych, jeżeli dane pochodzić mogą z różnych źródeł, identyfikatora użytkownika wprowadzającego dane, informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione, jeśli przewidziane jest udostępnianie danych innym podmiotom, chyba że dane te traktuje się jako dane powszechnie dostępne, sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 7 ustawy, po jego uwzględnieniu, oraz sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy. Natomiast zgodnie z § 17 rozporządzenia, system informatyczny służący do przetwarzania danych osobowych powinien umożliwić udostępnienie na piśmie, w powszechnie zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, wraz z informacjami, o których mowa w § 16 rozporządzenia.

Stwierdzone w wyniku kontroli naruszenie powyższych przepisów polegało na tym, iż system informatyczny nie zapewniał odnotowania, w przypadku „D" identyfikatora użytkownika wprowadzającego dane, natomiast w przypadku „A", „B" „C", „D", „E" oraz „F", informacji komu, kiedy i w jakim zakresie dane zostały udostępnione, a ponadto na braku możliwości udostępnienia na piśmie przez system informatyczny służący do przetwarzania danych osobowych, w przypadku „A", „B" „C", „D", „E" oraz „F", treści danych o każdej osobie, której dane są przetwarzane, wraz z informacją komu, kiedy i w jakim zakresie dane zostały udostępnione.

W piśmie z dnia […] sierpnia 2001 r. […]Kasa Chorych podnosi, że obowiązek zapewnienia, aby system informatyczny odnotował określone informacje, a następnie udostępniał je w formie pisemnej nie musi oznaczać wymogu wprowadzenia w odniesieniu do struktur baz danych i aplikacji nimi zarządzających odpowiednich opcji rejestrujących oraz umożliwiających wydrukowanie danych.

Nie można zaakceptować powyższego stanowiska […]KCh. Zawarte w § 16 i 17 rozporządzenia wymagania dotyczące możliwości odnotowania i udostępnienia na piśmie określonych danych w przypadku automatycznego przetwarzania danych należy bowiem odnosić do odpowiednich procedur programowych, a nie ludzi. Czynnik ludzki, o którym mowa w powołanej przez […]KCh definicji sytemu informatycznego, należy rozumieć pod kątem zagadnień związanych z zarządzaniem użytkownikami systemu i ich autoryzacją. Wymóg, aby treść danych o każdej osobie, której dane są przetwarzane, wraz z informacjami, o których mowa w § 16 rozporządzenia, była udostępniana na piśmie jest równoważny z wymogiem wytworzenia przez system informatyczny odpowiedniego pisma, tj. wydruku komputerowego.

Niezależnie od prezentowanego ww. stanowiska pismem z dnia […] września 2001 r, […]KCh poinformowała o usunięciu uchybienia polegającego na braku odnotowanie identyfikatora

użytkownika wprowadzającego dane osobowe do „D”. Wyjaśnienia […]KCh w powyższym zakresie należy uznać za wystarczające.

Ponadto oświadczono, że w pozostałym wskazanym w pkt 4 i 5 zawiadomienia o wszczęciu postępowania administracyjnego zakresie zostały podjęte działania mające na celu prawidłowe wypełnienie obowiązków określonych w § 16 i 17 rozporządzenia. W terminie trzech miesięcy wprowadzone zostaną funkcje zapewniające odnotowanie udostępnień danych osobowych, zintegrowane ze wszystkimi zbiorami wskazanymi w pkt 4 zawiadomienia o wszczęciu postępowania administracyjnego. Ponadto poinformowano, że w zbliżonym do powyższego terminie (do końca 2001 r.) wdrożona zostanie opcja zapewniająca odnotowywanie informacji wskazanych w pkt 5 ww. zawiadomienia, a także nowa wersja „B” spełniająca wymogi określone w § 16 i 17 rozporządzenia. Powyższe terminy usunięcia stwierdzonych uchybień uzasadniono złożonością systemu informatycznego eksploatowanego w […]KCh i związanym z tym zakresem koniecznych zmian technicznych i organizacyjnych.

Zgodnie z § 14 ust. 3 rozporządzenia, dla każdego użytkownika systemu informatycznego, w którym przetwarza się dane osobowe, administrator danych lub upoważniona przez niego osoba ustala odrębny identyfikator i hasło. Natomiast zgodnie z § 14 ust. 6 rozporządzenia, hasło użytkownika powinno być zmieniane co najmniej raz na miesiąc.

W toku kontroli ustalono, że jeden identyfikator i odpowiadające mu hasło dostępu do aplikacji „G” używany był przez dwóch użytkowników. Ponadto stwierdzono, że hasło dostępu do aplikacji „K” w przypadku jednego użytkownika systemu kadrowo - płacowego nie było zmieniane. W odniesieniu do ww. uchybień […]KCh pismem z dnia […] sierpnia 2001 r. poinformowała, że wskazane nieprawidłowości zostały usunięte. Wobec treści złożonych wyjaśnień należy uznać, że ustalony w toku kontroli stan faktyczny uległ zmianie i obecnie nie narusza obowiązującego w tym zakresie prawa.

Zgodnie z art. 39 ustawy, administrator danych zobowiązany jest prowadzić ewidencję osób zatrudnionych przy ich przetwarzaniu. Osoby te obowiązane są do zachowania danych w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia. Do powyższej ewidencji, zgodnie § 14 ust. 4 rozporządzenia, wpisuje się identyfikator ustalony dla każdego użytkownika systemu informatycznego wraz z imieniem i nazwiskiem użytkownika.

W wyniku kontroli ustalono, że […]Kasa Chorych jest administratorem zbioru o nazwie „G”. Zbiór ten prowadzony jest w systemie informatycznym „C”. W […]KCh prowadzona była ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w postaci spisu użytkowników obejmującego imiona, nazwiska i identyfikatory osób zarejestrowanych w domenie

NT. Spis ten nie zawierał jednak osób obsługujących system „C” w podmiotach udzielających świadczeń medycznych.

Jak wyżej przytoczono, w opinii […]Kasy Chorych administrator danych zobligowany jest jedynie do prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych u administratora.

Nie można zgodzić się z powyższym stanowiskiem. Z brzmienia art. 39 ustawy o ochronie danych osobowych nie wynika, aby obowiązek prowadzenia ewidencji dotyczył jedynie osób zatrudnionych „u administratora danych”. Obowiązek ten należy odnosić do wszystkich osób zatrudnionych przy przetwarzaniu danych w zbiorze prowadzonym przez określonego administratora danych, a tym samym do wszystkich osób mających dostęp do danych znajdujących się w tym zbiorze. Wskazuje na to sformułowanie zawarte w art. 39 ust. 2 ustawy „osoby, o których mowa w ust. 1, mające dostęp do danych osobowych”, jak również zobowiązanie administratora danych przetwarzanych w systemie informatycznym do zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, wynikające z art. 38 wskazanej ustawy. Za takim stanowiskiem przemawia również § 14 ust. 3 i 4 rozporządzenia, w których mowa jest o identyfikatorze, który powinien być ustalany dla każdego użytkownika systemu informatycznego. Prawidłowe dopełnienie obowiązku określonego w art. 39 ustawy ma na celu zapewnienie przez administratora danych właściwej ochrony przetwarzanych danych osobowych. Uznać zatem należy, że art. 39 ust. 1 ustawy o ochronie danych osobowych nakłada na […]KCh jako administratora zbioru o nazwie „G” obowiązek prowadzenia ewidencji obejmującej wszystkie osoby, które mają dostęp do danych przetwarzanych w powyższym zbiorze, zarówno pracowników […]KCh, jak i osoby obsługujące ten system u podmiotów świadczących usługi medyczne.

W piśmie z dnia […] sierpnia 2001 r. […]KCh oświadczyła, że rozpoczęto tworzenie ewidencji użytkowników systemu „C”, a następnie pismem z dnia […] września 2001 r. poinformowała, że obecnie prowadzony jest wykaz obejmujący wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych. Również przytoczone wyżej wyjaśnienia dotyczące zakresu informacji o użytkownikach systemu informatycznego, potwierdzone załączonym do pisma wydrukiem komputerowym należy uznać za wystarczające dla uznania, że uchybienie wskazane w pkt 3 zawiadomienia o wszczęciu postępowania administracyjnego zostało usunięte.

Stosownie do art. 105 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (tekst jednolity: Dz. U. z 2000 r., Nr 98, poz. 1071), gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o umorzeniu postępowania. Ze względu na to, że zostały usunięte uchybienia w procesie przetwarzania danych osobowych wskazane w pkt 1, 2 i 3 zawiadomienia o wszczęciu postępowania administracyjnego oraz uchybienie polegające na tym, iż system informatyczny nie

zapewniał odnotowania identyfikatora użytkownika wprowadzającego dane w przypadku „D”, należało umorzyć postępowanie w tym zakresie.

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja niniejsza jest ostateczna. Strona niezadowolona z tej decyzji, na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych i art. 129 § 2 kodeksu postępowania administracyjnego, może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: 00-030 Warszawa, PI. Powstańców Warszawy 1) z wnioskiem o ponowne rozpatrzenie sprawy w terminie 14 dni od dnia otrzymania niniejszej decyzji.