



GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH

*Michał Serzycki*

Warszawa, dnia 7 kwietnia 2008 r.

DIS/DEC – **222/8731/08** dot.

DIS-K-421/147/07 DIS-K-

421/149/07

**DECYZJA**

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 i art. 22 w związku z art. 36 ust. 1 i 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 § 4 pkt 1 i pkt 4, § 5, § 7 ust. 1 pkt 1, pkt 2 i 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 część A pkt II ust. 1 i pkt III ppkt 1 załącznika do rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Archiwum X.

## **I. Nakazuję Archiwum X**

**usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:**

### **1. Zmodyfikowanie systemów informatycznych o nazwach: „X” (służącego do ewidencji użytkowników zasobu archiwalnego udostępnianego w pracowni naukowej,**

**ewidencjonowania reprografii oraz ewidencjonowania osób odwiedzających pracownię naukową) i „Y” (służącego do rejestrowania pism przychodzących), użytkowanych w ArchiwumX, w taki sposób, aby systemy te zapewniały, dla każdej osoby, której dane są przetwarzane w tych systemach odnotowanie daty pierwszego wprowadzenia danych do tych systemów oraz identyfikatorów użytkowników wprowadzających dane osobowe do ww. systemów (§ 7 ust. 1 pkt 1 i 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), w terminie 6 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**

### **2. Zmodyfikowanie systemów informatycznych o nazwach: „X” (służącego do ewidencji użytkowników zasobu archiwalnego udostępnianego w pracowni naukowej, ewidencjonowania reprografii oraz ewidencjonowania osób odwiedzających pracownię naukową) i „Y” (służącego do rejestrowania pism przychodzących), użytkowanych w Archiwum X w taki sposób, aby systemy te zapewniały, dla każdej osoby, której dane są przetwarzane w tych systemach sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemów oraz identyfikatorze użytkownika wprowadzającego dane do systemów (§ 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 ), w terminie 6 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**

**II. W pozostałym zakresie postępowanie umarzani.**

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w: Archiwum X (sygn. akt DIS-K-421/147/07) oraz w oddziale tego Archiwum X (sygn. akt DIS-K-421/149/07), 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 pracowników ww. podmiotów ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokołach kontroli, które zostały podpisane odpowiednio przez Dyrektora Archiwum X jak również Kierownika oddziału Archiwum X.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych, Archiwum X, jak również oddział Archiwum naruszyły przepisy o ochronie danych osobowych. Administratorem danych przetwarzanych przez ww. podmioty jest Archiwum X. Uchybienia polegały na:

1. Niezastosowaniu zgodnie z art. 36 ust. 1 ustawy odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności nie zabezpieczeniu danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną.

W Archiwum X pomimo, iż zgodnie z zapisem § 4 „Regulaminu korzystania z materiałów archiwalnych w pracowni naukowej Archiwum X użytkownicy są zobowiązani do posługiwania się w pomieszczeniach archiwum kartą identyfikacyjną, karty te nie są stosowane.

2. Niezapewnieniu przez administratora danych zgodnie z art. 38 ustawy, kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone, gdyż systemy informatyczne o nazwach: „X” (służącego do ewidencji użytkowników zasobu archiwalnego udostępnianego w pracowni naukowej, ewidencjonowania reprografii oraz ewidencjonowania osób odwiedzających pracownię naukową) i „Y” (służącego do rejestrowania pism przychodzących) użytkowane w Archiwum X, nie odnotowują dla każdej osoby, której dane osobowe są przetwarzane w tych systemach, daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 1 pkt 1 i pkt 2 rozporządzenia).

3. Niezapewnieniu, aby systemy informatyczne o nazwach: „X” i „Y” użytkowane w Archiwum X, umożliwiały dla każdej osoby, której dane osobowe są przetwarzane w tych systemach, sporządzanie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których

mowa w § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia, tj. datę pierwszego wprowadzenia danych do systemu, identyfikator użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 3 rozporządzenia).

4. Niezawarcu przez Archiwum X, zgodnie z treścią § 4 pkt 1 i pkt 4 rozporządzenia, w polityce bezpieczeństwa informacji w zakresie wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe i opisu sposobu przepływu danych pomiędzy systemami informatycznymi o nazwach: „SEZAM” (system ewidencji zasobu archiwalnego), „Algorytm” (służący do przetwarzania danych finansowo-księgowych), „Eksplorator VideoTel” (służący do dokonywania przelewów bankowych) i „WF-Gang” (system służący do przetwarzania danych kadrowo-płacowych).
5. Niezawarcu przez Archiwum X w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zgodnie z § 5 rozporządzenia, informacji dotyczących użytkowanych przez ten podmiot systemów informatycznych o nazwach: „SEZAM”, „Algorytm”, „Eksplorator VideoTel” i „WF-Gang”.
6. Niezabezpieczeniu, zgodnie z częścią A, pkt II ust. 1 załącznika do rozporządzenia, dostępu do systemu informatycznego o nazwie „SEZAM” (użytkowanego lokalnie, na komputerze znajdującym się w Archiwum X za pomocą mechanizmu uwierzytelnienia (logowania)).
7. Niezabezpieczeniu, zgodnie z częścią A, pkt III ppkt 1 załącznika do rozporządzenia, komputera, znajdującego się w pomieszczeniu nr 102 w budynku Archiwum X, na którym użytkowany jest system informatyczny o nazwie „SEZAM” poprzez zainstalowanie oprogramowania antywirusowego.
8. Niezabezpieczeniu, zgodnie z częścią A, pkt III ppkt 1 załącznika do rozporządzenia, w Archiwum X i w jego oddziale, stacji roboczych, na których znajdują się systemy informatyczne służące do przetwarzania danych osobowych o nazwach: „X” (służącego do udostępnienia materiałów archiwalnych) oraz „Y” (służącego do rejestrowania pism przychodzących) poprzez zainstalowanie oprogramowania antywirusowego.

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w stosunku do Archiwum X jako administratora danych (strony postępowania) w celu wyjaśnienia okoliczności sprawy.

Pismem z dnia 5 lutego 2008 r. (sygn. DIS-K-421/147/07/2842/08, sygn. DIS-K-421/149/07/2842/08), zawiadamiającym o wszczęciu postępowania administracyjnego

w przedmiotowej sprawie, 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 Archiwum X pismami z dnia 13 lutego 2008 r. (sygn. 070-1/07) i z dnia 7 marca 2008 r. (sygn. 070-1/2008) przesłał wyjaśnienia w zakresie stwierdzonych uchybień oraz dowody mające potwierdzić ich usunięcie. Ze złożonych wyjaśnień wynika, iż:

1. Dyrektor Archiwum X Aneksiem z dnia 22 listopada 2007 r. do Zarządzenia nr 2 Dyrektora Archiwum X z dnia 29 czerwca 2000 r. wprowadził zmiany w „Regulaminie korzystania z materiałów archiwalnych w pracowni naukowej Archiwum X poprzez wykreślenie z ww. Regulaminu § 4, który dotyczył konieczności posługiwania się w pomieszczeniach archiwum kartą identyfikacyjną.
2. W przypadku braku identyfikatora osoby wprowadzającej dane osobowe do systemu, jak również braku możliwości sporządzenia i wydrukowania raportu wyjaśniono, iż w zakresie systemu informatycznego o nazwie "X" Archiwum X nie posiada możliwości ingerowania w konstrukcję ww. systemu, gdyż jest to baza ogólnokrajowa przekazana do stosowania przez Naczelną Dyрекcję Archiwów. Natomiast, w przypadku systemu informatycznego o nazwie „Y” wyjaśniono, iż trwają prace nad automatycznym generowaniem identyfikatora osoby wprowadzającej dane osobowe do systemu oraz stosownego raportu. Ponadto, wyjaśniono, iż do czasu wdrożenia ww. rozwiązania dane do systemu wprowadza wyłącznie jedna, upoważniona osoba.
3. W zakresie braku w polityce bezpieczeństwa wykazu budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe wyjaśniono, iż z dniem 11 lutego 2008 r. wprowadzono Aneks do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Archiwum X, w którym, w załączniku nr 9 określono wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe. Natomiast, w zakresie opisu przepływu danych pomiędzy systemami informatycznymi dodano do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Archiwum X załącznik nr 5, o tytule „Opis struktur i sposoby przepływu danych pomiędzy systemami”, w którym opisano sposób przepływu danych pomiędzy systemami informatycznymi o nazwach: „PŁATNIK”, „ProgMan - KADRY”, „ProgMan - PŁACE”, „Eksplorator Video Tel”. Odnosnie informacji dotyczących użytkowanych przez Archiwum X systemów informatycznych wyjaśniono, iż do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Archiwum X

dodano wykaz baz danych o nazwach: „PŁATNIK”, „ProgMan - KADRY”, „ProgMan - PŁACE”, „Eksplorator Video Tel”. Ponadto, wyjaśniono, iż w przypadku systemów informatycznych o nazwach: „ALGORTYM”, „WF-GANG” z dniem 1 stycznia 2008 r. zaprzestano stosowania ww. systemów w Archiwum X.

4. Odnośnie zabezpieczenia (zgodnie z częścią A, pkt II ust. 1 załącznika do rozporządzenia) dostępu do systemu informatycznego o nazwie „SEZAM” za pomocą mechanizmu uwierzytelnienia (logowania) jak również w zakresie zabezpieczenia (zgodnie z częścią A, pkt III ppkt 1 załącznika do rozporządzenia) ww. systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego wyjaśniono, iż system informatyczny o nazwie „SEZAM” został usunięty z komputera znajdującego się w pomieszczeniu nr 102 w budynku Archiwum X.

5. W zakresie braku zabezpieczenia przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (zgodnie z częścią A, pkt III ppkt 1 załącznika do rozporządzenia) wyjaśniono, iż w oddziale Archiwum X na stacjach roboczych, na których znajdują się systemy informatyczne służące do przetwarzania danych osobowych o nazwach „X” oraz „Y” zostało zainstalowane oprogramowanie antywirusowe.

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

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 zgodnie z § 7 ust. 1 pkt 1 i 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: 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. Ponadto, 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 § 7 ust. 1. rozporządzenia.

W toku kontroli ustalono, iż w odniesieniu do systemów informatycznych o nazwach: „X” (służącego do ewidencji użytkowników zasobu archiwalnego udostępnianego w pracowni naukowej, ewidencjonowania reprografii oraz ewidencjonowania osób odwiedzających





pracownię naukową) i „Y” (służącego do rejestrowania pism przychodzących) użytkowanych w Archiwum X nie została zapewniona kontrola nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone. W toku czynności kontrolnych ustalono, że ww. systemy informatyczne nie zapewniają odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane do tych systemów informatycznych, jak również nie zapewniają sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje w zakresie identyfikatora użytkownika wprowadzającego dane do systemu informatycznego.

Z wyjaśnień złożonych przez Dyrektora Archiwum X wynika, iż system informatyczny o nazwie „X” został przekazany do użytkowania w Archiwum X przez Naczelną Dyрекcję Archiwów i w związku z tym Archiwum X nie ma możliwości ingerencji w jego konstrukcję.

Odnosząc się do ww. wyjaśnień, stwierdzić należy, iż Archiwum X jako administrator danych osobowych przetwarzanych w ww. systemie jest zobligowane do dopełnienia obowiązków określonych przepisami o ochronie danych osobowych, w tym również, o których mowa w § 7 ust. 1 pkt 1, pkt 2 i § 7 ust. 3 rozporządzenia.

Natomiast, Dyrektor Archiwum X wyjaśnił, iż w przypadku systemu informatycznego o nazwie „Y” trwają prace nad automatycznym generowaniem identyfikatora osoby wprowadzającej dane do tego systemu jak również możliwością generowania przez ten system stosownego raportu.

Wobec powyższego uznać należy, że uchybienia dotyczące systemów informatycznych o nazwie „X” i „Y” użytkowane w Archiwum, we wskazanym wyżej zakresie nie zostały usunięte, a zatem wyznaczony został odpowiedni termin do przywrócenia w tym zakresie stanu zgodnego z prawem.

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

1. Zastosowano środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust.1 ustawy o ochronie danych osobowych), tj. wprowadzono zmiany

w treści „Regulaminu korzystania z materiałów archiwalnych w pracowni naukowej Archiwum X i obecnie nie ma obowiązku posługiwania się w pomieszczeniach archiwum kartą identyfikacyjną.

2. Uzupełniono politykę bezpieczeństwa w zakresie: 1) wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe - § 4 pkt 1 rozporządzenia, 2) sposobu przepływu danych pomiędzy poszczególnymi systemami, w zakresie informacji dotyczących systemu informatycznego o nazwie: „Eksplorator VideoTel” (służący do dokonywania przelewów bankowych) - § 4 pkt 4 rozporządzenia.

3. Uzupełniono instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w zakresie: informacji dotyczących użytkowanego przez Archiwum X systemu informatycznego o nazwie „Eksplorator VideoTel” (służący do dokonywania przelewów bankowych) - § 5 rozporządzenia.

Natomiast, wyjaśniono, iż system informatyczny o nazwie „SEZAM” (system ewidencji zasobu archiwalnego) został przez Archiwum X usunięty i nie są w nim przetwarzane dane osobowe. Ponadto, poinformowano, iż z dniem 1 stycznia 2008 r. zaprzestano stosowania w Archiwum X systemów informatycznych o nazwach: „ALGORTYM” (służący do przetwarzania danych finansowo-księgowych) i „WF - GANG” (system służący do przetwarzania danych kadrowo-płacowych).

4. Odnośnie zabezpieczenia dostępu do systemu informatycznego o nazwie „SEZAM” za pomocą mechanizmu uwierzytelnienia (logowania) - (zgodnie z częścią A, pkt II ust. 1 załącznika do rozporządzenia) jak również zainstalowania oprogramowania antywirusowego (zgodnie z częścią A, pkt III ppkt 1 załącznika do rozporządzenia) wyjaśniono, iż system ten został przez Archiwum X usunięty i nie są w nim przetwarzane dane osobowe.

5. Zabezpieczeniu (zgodnie z częścią A, pkt III ppkt 1 załącznika do rozporządzenia), w oddziale Archiwum X stacji roboczych, na których znajdują się systemy informatyczne służące do przetwarzania danych osobowych o nazwach „X” oraz „Y” poprzez zainstalowanie programu antywirusowego.

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/Szl 029/97).

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.



