



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*Michał Serzycki*

Warszawa, dnia 27 maja 2010 r.

DIS/DEC - 652/21890/10

dot. DIS-K-421/29/10

**D E C Y Z J A**

Na podstawie art. 104 § 1, 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 ust. 2, 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 2, pkt 3, pkt 4, pkt 5, § 5, § 7 ust. 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 częścią A pkt II ust. 2 lit. a, pkt III ppkt 1 i ppkt 2, pkt IV ust. 2 i częścią B pkt VIII załącznika do ww. rozporządzenia po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez uczelnię wyższą,

**I. Nakazuję uczelni wyższej, usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:**

**1. Zmodyfikowanie systemu informatycznego o nazwie „X” (służącego do przetwarzania danych osobowych pracowników i studentów) oraz systemu informatycznego o nazwie „Y” (służącego do przetwarzania danych osobowych pracowników) tak, aby dla każdej osoby, której dane osobowe są w nich przetwarzane, systemy te zapewniały odnotowanie**

**identyfikatora użytkownika wprowadzającego dane osobowe do tych systemów, w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**

**2. Zmodyfikowanie systemu informatycznego o nazwie „X” (służącego do przetwarzania danych osobowych pracowników i studentów) oraz systemu informatycznego o nazwie „Y” (służącego do przetwarzania danych osobowych pracowników) tak aby dla każdej osoby, której dane osobowe są w nich przetwarzane, systemy te zapewniały sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o identyfikatorze użytkownika wprowadzającego dane osobowe do tych systemów, w terminie miesiąca 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 w uczelni wyższej (zwanej dalej także Uczelnią), kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. akt DIS- K- 421/29/10), 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 Uczelni ustne wyjaśnienia oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Rektora uczelni wyższej.

Ponadto dnia 4 marca 2010 r. uczelnia wyższa złożyła w Biurze Generalnego Inspektora Ochrony Danych Osobowych kopię Zarządzenia nr 9/2010 Rektora uczelni w sprawie „Polityki Bezpieczeństwa w zakresie ochrony danych osobowych w uczelni” oraz kopię Zarządzenia nr 10/2010 Rektora uczelni w sprawie „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w uczelni” (powołane dokumenty zostały załączone do akt sprawy).

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych uczelnia wyższa, jako administrator danych, naruszyła przepisy o ochronie danych osobowych, tj.:

1. Uczelnia jako administrator danych nie zastosowała środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń (art. 36 ust. 1 ustawy), tj.:

1.1. System informatyczny o nazwie „X” służący do przetwarzania danych osobowych pracowników i studentów uczelni, nie zapewniał aby dla każdego użytkownika rejestrowany był odrębny identyfikator. W systemie tym założone były konta dla dwóch użytkowników. Z kont tych faktycznie korzystało ośmiu użytkowników (część A pkt II ust. 2 lit. a załącznika do rozporządzenia),

1.2. System informatyczny o nazwie „Y” służący do przetwarzania danych osobowych studentów uczelni nie był zabezpieczony przed utratą danych spowodowanych awarią zasilania (część A pkt III ppkt 1 i ppkt 2 załącznika do rozporządzenia),

1.3. Hasło do systemu informatycznego o nazwie „X” służącego do przetwarzania danych osobowych pracowników i studentów uczelni w ogóle nie było zmieniane (część A pkt IV ust. 2 załącznika do rozporządzenia),

1.4. Do uwierzytelniania użytkowników w systemie informatycznym o nazwie „X” służącym do przetwarzania danych osobowych pracowników i studentów uczelni, używano hasła, które składało się z sześciu znaków i zawierało tylko małe litery (część B pkt VIII załącznika do rozporządzenia),

2. Dokumentacja opisująca sposób przetwarzania danych osobowych w uczelni oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych była niekompletna (art. 36 ust. 2 ustawy), tj.

2.1. Polityka bezpieczeństwa uczelni wyższej wprowadzona Zarządzeniem nr 9/2010 Rektora Uczelni Wyższej w sprawie Polityki Bezpieczeństwa w zakresie ochrony danych osobowych w uczelni wyższej, nie zawierała:

- wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (§ 4 pkt 2 rozporządzenia),
- opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (§ 4 pkt 3 rozporządzenia),
- sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 4 rozporządzenia),
- określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (§ 4 pkt 5 rozporządzenia).

2.2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych uczelni wprowadzona Zarządzeniem nr 10/2010 Rektora uczelni w sprawie Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w uczelni, nie zawierała:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności,
- informacji o stosowanych metodach i środkach uwierzytelnienia oraz procedury związanej z ich zarządzaniem i użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonej dla użytkowników systemu,
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
- informacji o sposobie, miejscu i okresie przechowywania,
- a) informacji o elektronicznych nośnikach informacji zawierających dane osobowe,
- b) informacji o kopiach zapasowych, o których mowa w pkt 4 rozporządzenia,
- informacji o sposobie zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,
- informacji o sposobie realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia,
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (§5 rozporządzenia).

3. System informatyczny o nazwie „X” służący do przetwarzania danych osobowych pracowników i studentów uczelni i system informatyczny o nazwie „Y” służący do przetwarzania danych osobowych pracowników uczelni (system kadrowo-płacowy) dla każdej osoby, której dane osobowe były przetwarzane, nie zapewniały odnotowania identyfikatora użytkownika wprowadzającego dane do systemu oraz nie zapewniały sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia, tj. identyfikatora użytkownika wprowadzającego dane do systemu (art. 38 ustawy w związku z § 7 ust. 1 pkt 2 i ust. 3 rozporządzenia).

W związku z powyższym, w dniu 31 marca 2010 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma DIS-K-421/29/10/13783).

Pismem z dnia 13 kwietnia 2010 r. stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego Uczelnia Wyższa poinformowała, iż:

1. Do chwili zakupu nowej wersji systemu informatycznego o nazwie „X” służącego do przetwarzania danych osobowych pracowników i studentów uczelni, umożliwiającą założenie kont dla wszystkich jego użytkowników, z systemu tego korzystać będą tylko pracownicy Biblioteki uczelni posiadający konta.

2. W celu zabezpieczenia systemu informatycznego o nazwie „T” służącego do przetwarzania danych osobowych studentów uczelni przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, w trakcie realizacji jest zakup zasilacza zapasowego UPS.
3. Zabezpieczając przed nieautoryzowanym dostępem do baz danych systemu informatycznego o nazwie „X” służącego do przetwarzania danych osobowych pracowników i studentów uczelni, zastosowano wymuszenie zmiany hasła co 30 dni.
4. Hasło służące do uwierzytelnienia użytkowników systemu informatycznego o nazwie „X,, za pomocą którego przetwarzane są dane osobowe pracowników i studentów uczelni składa się obecnie z 8 znaków i zawiera małe i wielkie litery, cyfry oraz znaki specjalne,
5. Zarządzeniem nr 14/2010 z dnia 26 marca 2010 r. Rektor Uczelni Wyższej uzupełnił politykę bezpieczeństwa uczelni o:
  - 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.
6. Zarządzeniem nr 15/2010 Rektora Uczelni Wyższej zostały wprowadzone zmiany do Polityki Bezpieczeństwa w zakresie ochrony danych w uczelni polegające na dopisaniu nowego Rozdziału VII – Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
7. Zarządzeniem nr 16/2010 Rektora Uczelni Wyższej z dnia 12 kwietnia 2010 r. wprowadzono nową Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w uczelni.
8. W systemie informatycznym o nazwie „X” służącym do przetwarzania danych osobowych pracowników i studentów uczelni i systemie informatycznym o nazwie „Y” służącym do przetwarzania danych osobowych pracowników uczelni (system kadrowo-płacowy) nie ma obecnie możliwości odnotowania identyfikatora użytkownika wprowadzającego dane do systemu ani sporządzania i drukowania raportów zawierających informacje na ten temat. Jednocześnie w piśmie z dnia 13 kwietnia 2010 r. Rektor uczelni zapewnił, iż w nowej wersji systemu informatycznego o nazwie „X”, która zostanie zakupiona w maju 2010 r. będzie już taka możliwość. Ponadto w ww. piśmie Rektor uczelni poinformował Generalnego Inspektora Ochrony Danych Osobowych, iż zaplanowano także zakup nowej wersji systemu kadrowo-płacowego o nazwie „Safo”, który będzie sfinalizowany do końca czerwca 2010 r.. Nowa wersja systemu o nazwie „Y” będzie spełniała wszystkie wymagania związane z ochroną danych osobowych.

Na dowód powyższego do pisma z dnia 13 kwietnia 2010 r. Rektor uczelni załączył: kopię Zarządzenia nr 14/2010 Rektora uczelni w sprawie wykazu zbiorów, w których przetwarzane są dane osobowe w Uczelni Wyższej, kopię Zarządzenia nr 15/2010 Rektora uczelni w sprawie wprowadzenia zmian w Polityce Bezpieczeństwa w zakresie ochrony danych osobowych w uczelni oraz kopię Zarządzenia nr 16/2010 Rektora uczelni w sprawie Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w uczelni.

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

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. Stosownie do § 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.

W toku kontroli ustalono, że system informatyczny o nazwie „X”, w którym są przetwarzane dane osobowe pracowników i studentów uczelni oraz system informatyczny o nazwie „Y”, w którym są przetwarzane dane osobowe pracowników uczelni, nie zapewniają dla każdej osoby, której dane osobowe są w nich przetwarzane, odnotowania identyfikatora użytkownika wprowadzającego dane oraz sporządzenia i wydrukowania raportu zawierającego informacje o identyfikatorze użytkownika wprowadzającego dane osobowe.

Jednocześnie należy wskazać, iż Generalny Inspektor uwzględniając wyjaśnienia strony dotyczące podjęcia działań zmierzających do przywrócenia stanu zgodnego z prawem, wyznaczył miesięczny termin wykonania niniejszej decyzji.

Na podstawie złożonych przez Uczelnię pisemnych wyjaśnień oraz przedstawionych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.:

1. Obecnie z systemu informatycznego o nazwie „X” służącego do przetwarzania danych osobowych pracowników i studentów uczelni korzystają, tylko użytkownicy posiadający identyfikatory,
2. Została uruchomiona procedura mająca na celu zakup zasilacza awaryjnego UPS, w celu zabezpieczenia systemu o nazwie „T” służącego do przetwarzania danych osobowych studentów uczelni przed utratą danych spowodowaną awarią zasilania,
3. W systemie informatycznym o nazwie „X” służącym do przetwarzania danych osobowych pracowników i studentów uczelni, wymuszenie hasła następuje co 30 dni a hasło składa się w chwili obecnej z 8 znaków i zawiera małe i wielkie litery,

4. Z analizy Zarządzenia nr 14/2010 Rektora Uczelni Wyższej w sprawie wykazu zbiorów, w których przetwarzane są dane osobowe w uczelni, Zarządzenia nr 15/2010 Rektora uczelni w sprawie wprowadzenia zmian w Polityce Bezpieczeństwa w zakresie ochrony danych osobowych w uczelni oraz Zarządzenia nr 16/2010 Rektora uczelni w sprawie Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w uczelni (załączonych do pisma z dnia 13 kwietnia 2010 r. stanowiącego odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego) wynika, iż obecnie polityka bezpieczeństwa uczelni spełnia wymogi § 4 rozporządzenia a Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w uczelni spełnia wymogi § 5 rozporządzenia.

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 Kodeksu postępowania administracyjnego jest bezprzedmiotowość postępowania „z jakiegokolwiek 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. SA/Sz1029/97).

Na podstawie całokształtu materiału dowodowego zebranego w niniejszej sprawie uznać należy, iż w toku postępowania usunięte zostały uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania i dlatego należało je w tej części umorzyć.

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.