M O N I T O R
UNIWERSYTETU WARSZAWSKIEGO

Poz. 97

ZARZĄDZENIE NR 9
REKTORA UNIWERSYTETU WARSZAWSKIEGO

z dnia 1 września 2004 r.

w sprawie ochrony danych osobowych w Uniwersytecie Warszawskim

Na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U z 2002 r. Nr 101 poz. 926 z późn. zm.) zwanej dalej ustawą i § 3 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), zwanego dalej rozporządzeniem, oraz § 65 Statutu Uniwersytetu Warszawskiego zarządza się, co następuje:

§ 1

1. Administratorem danych osobowych (ADO) Uniwersytetu Warszawskiego jest Dyrektor Administracyjny, który powołuje Administratorów Bezpieczeństwa Informacji (ABI).

2. ABI są powoływani na wniosek:

a) dziekana,
b) Dyrektora Administracyjnego w odniesieniu do wszystkich jednostek administracji centralnej,
c) Dyrektora BUW,
d) Dyrektora ICM dla wszystkich pozostałych jednostek organizacyjnych.

3. ABI są odpowiedzialni za realizację zadań administratora danych osobowych określonych w ustawie, w odniesieniu do zbiorów danych istniejących w danej jednostce organizacyjnej UW.

§ 2

ABI podejmują niezbędne działania służące realizacji zabezpieczenia danych osobowych przetwarzanych w poszczególnych zbiorach, a w szczególności powinni:

1) zapewnić stosowanie środków technicznych i organizacyjnych, o których mowa w art. 36 ust. 1 ustawy, zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
2) zapewnić stosowanie środków bezpieczeństwa, o których mowa w § 6 ust. 5 rozporządzenia;

3) dostosować w terminie określonym w § 9 rozporządzenia urządzenia i systemy informatyczne służące do przetwarzania danych osobowych do warunków określonych w rozporządzeniu;
4) zapewnić prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa w pkt 1 i 2.

§ 3

1. ABI są zobowiązani do przekazania ADO do końca 2004 r. następujących informacji:
1) wykazu baz danych w systemach informatycznych i innych zbiorów danych, w których przetwarzane są dane osobowe według wzoru stanowiącego załącznik nr 1 do niniejszego zarządzenia;
2) ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych i ich identyfikatorów według wzoru stanowiącego załącznik nr 2 niniejszego zarządzenia,
3) wykazu miejsc, w których przetwarza się dane osobowe według wzoru stanowiącego załącznik nr 3 niniejszego zarządzenia.

2. ABI, działając zgodnie z instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie Warszawskim, stanowiącą załącznik nr 4 do niniejszego zarządzenia, opracowują szczegółowe instrukcje zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w zbiorach danych istniejących w danej jednostce organizacyjnej UW.

3. ABI są zobowiązani do informowania ADO o wszystkich zmianach informacji przekazanych ADO zawartych w wyżej wymienionych załącznikach.

§ 4

ABI są zobowiązani do działania zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych w Uniwersytecie Warszawskim stanowiącą załącznik nr 5 do niniejszego zarządzenia oraz opracowania do końca 2004 r. szczegółowych instrukcji w tym przedmiocie w odniesieniu do zbiorów danych istniejących w danej jednostce organizacyjnej UW.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor UW: *P. Węgleński*

Załącznik nr 1
do Zarządzenia nr 9 Rektora UW
z dnia 1 września 2004 r.

.....
nazwa jednostki organizacyjnej

.....
Administrator Bezpieczeństwa Informacji

Wykaz baz danych w systemach informatycznych i innych zbiorów danych w których przetwarzane są dane osobowe na Uniwersytecie Warszawskim

Lp.	Nazwa bazy danych	System bazy danych/System operacyjny serwera [1]	Sposób archiwizowania i zabezpieczenia informatycznego [2]	Zawiera także dane osób spoza UW (T/N)	Liczba miejsc przetwarzania i liczba porządkowa zał. nr 3

[1] np. plik Excel/WIN, baza MySQL/Netware 6.5, Oracle/AIX,
[2] np. (A) archiwum, (B) backup, (F) wydzielona fizycznie sieć (I) indywidualne hasło, (S) szyfrowanie, (U) UPS,

Załącznik nr 2
do Zarządzenia nr 9 Rektora UW
z dnia 1 września 2004 r.

.....
nazwa jednostki organizacyjnej

.....
Administrator Bezpieczeństwa Informacji

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów

Lp.	Nazwa bazy danych[(1)]	Nazwisko i imię użytkownika	Nazwa identyfikatora	Rodzaj uprawnień[(2)]	Lokalizacja [(3)]	Uwagi

[(1)]nazwa bazy danych z zał. nr 1,
[(2)]skróty: (A) prawo do wykonywania kopii, (D) prawo do drukowania, (N) prawo do zakładania nowych kont, (M) prawo do dodawania i modyfikacji danych, (P) prawo do przeglądania danych na ekranie, Uwaga: prawa do części bazy danych sygnalizować w polu Uwagi,
[(3)]zgodnie z zał. nr 3,

Załącznik nr 3
do Zarządzenia nr 9 Rektora UW
z dnia 1 września 2004 r.

.....
nazwa jednostki organizacyjnej

.....
Administrator Bezpieczeństwa Informacji

Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych na Uniwersytecie Warszawskim

Lp.	Nazwa bazy danych[(1)]	Lokalizacja (adres)	Nr pokoju/piętro	Funkcja lokalizacji[(2)]	Zabezpieczenie fizyczne[(3)]

[(1)] z Załącznika nr 1,
[(2)] np. (A) pomieszczenie admin. baz danych, (K) miejsce przechowywania kopii bezp., (S) serwer, (U) pomieszczenie osób wprowadzających dane osobowe, (Z) pomieszczenie, w którym wykonywane są kopie bezpieczeństwa,

Załącznik nr 4
do Zarządzenia nr 9 Rektora UW
z dnia 1 września 2004 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji

Niniejsza instrukcja określa ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych na Uniwersytecie Warszawskim oraz stanowi podstawę do opracowania instrukcji szczegółowych uwzględniających specyfikę poszczególnych systemów informatycznych funkcjonujących w uczelni.

§ 1

Administrator bezpieczeństwa informacji (ABI) UW:

1) czuwa nad wdrażaniem niniejszej instrukcji w systemach informatycznych Uniwersytetu Warszawskiego, w których przetwarzane są dane osobowe oraz dba o bieżące jej uaktualnianie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych uczelni,
2) określa politykę bezpieczeństwa systemów informatycznych w uczelni,
3) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych uczelni,
4) określa potrzeby w zakresie zabezpieczenia systemów informatycznych w których przetwarzane są dane osobowe,
5) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych oraz ich przetwarzania.

§ 2

ABI stwarza właściwe warunki organizacyjno-techniczne gwarantujące bezpieczeństwo systemów informatycznych (w miarę możliwości finansowo-lokalowych UW), a w szczególności:

1) wyznacza tam gdzie jest to niezbędne administratorów poszczególnych systemów informatycznych i wraz z nimi tworzy szczegółową instrukcję zarządzania systemami informatycznymi,
2) nadzoruje wyznaczonych administratorów w zakresie:
   a) lokalizacji pomieszczeń, w których przetwarzane są dane osobowe,
   b) lokalizacji pomieszczeń, w których przechowywane są kopie awaryjne zbiorów danych osobowych,
   c) instalowania krat i systemów alarmowych adekwatnych do zagrożenia systemów informatycznych,
   d) zakupu systemów operacyjnych, baz danych, oprogramowania antywirusowego oraz systemów kryptograficznych podnoszących bezpieczeństwo danych osobowych oraz gwarantujących spełnienie wymogów określonych ustawą,
   e) zakupu pamięci masowych, pamięci taśmowych oraz innych urządzeń i nośników umożliwiających wykonywanie kopii zapasowych danych osobowych w systemach informatycznych,

f) właściwego prowadzenia i zabezpieczenia okablowania sieci komputerowej służącej do przetwarzania danych osobowych w systemach informatycznych w celu wyeliminowania niebezpieczeństwa podsłuchu lub zniszczenia infrastruktury sieciowej,
g) tworzenia bezpiecznego systemu energetycznego zasilającego system informatyczny,
h) zakupu niszczarek do dokumentów do pomieszczeń w których generowane są wydruki zawierające dane osobowe,
i) zakupu szaf pancernych do przechowywania kopii zapasowych danych osobowych z systemów informatycznych,
j) wdrażania technologii minimalizującej zagrożenie uzyskania dostępu do sieci osobom nieupoważnionym,
k) zakupu oprogramowania umożliwiającego rejestrowanie identyfikatorów i czas logowania użytkowników sieci,
l) nadzoru monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych,
m) określania sposobu przydziału haseł dla użytkowników poszczególnych systemów informatycznych i częstotliwości ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności,
n) określania sposobu rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności,
o) wyboru procedury rozpoczęcia i zakończenia pracy,
p) metody i częstotliwości wykonywania kopii awaryjnych,
q) metody i częstotliwości sprawdzania systemów informatycznych na obecność wirusów komputerowych oraz metody ich usuwania,
r) sposobu i czasu przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
s) sposobu postępowania w zakresie komunikacji w sieci komputerowej.

3) zabezpiecza budynki oraz pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych przed dostępem osób niepowołanych, a w szczególności:
   a) wprowadza i nadzoruje bieżącą aktualizację listy osób upoważnionych do pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe,
   b) wprowadza ewidencję osób pobierających klucz do pomieszczeń, w których przetwarzane są dane osobowe zawierającą m.in. czas pobierania i zdawania kluczy,
   c) określa tryb szkolenia portierów w budynkach, w których przetwarzane są dane osobowe w systemach informatycznych,
   d) określa tryb szkolenia osób sprzątających pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych uwzględniający specyfikę konserwacji systemów komputerowych.

4) Określa zasady i ewidencję wykonywania czynności serwisowych w systemach informatycznych w podległych jednostkach w celu wyeliminowania:
   a) możliwości wykonania kopii danych osobowych przez osoby nieupoważnione,
   b) przemieszczania urządzeń komputerowych i ich części służących do przetwarzania danych osobowych poza obszar objęty ochroną,
   c) podmiany elementów sprzętu komputerowego lub oprogramowania na inny, który zawiera cechy ukryte.

Załącznik nr 5
do Zarządzenia nr 9 Rektora
UW z dnia 1 września 2004 r.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Uniwersytecie Warszawskim

§ 1

Instrukcja niniejsza ma zastosowanie w sytuacjach:
1) stwierdzonego naruszenia zabezpieczenia (ew. ochrony) danych osobowych w systemie informatycznym lub innym zbiorze danych;
2) podejrzenia naruszenia zabezpieczenia (ew. ochrony) danych osobowych w systemie informatycznym lub innym zbiorze danych.

§ 2

Naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych stwierdza się, gdy wystąpiły między innymi:
1) nieuprawniony dostęp do danych osobowych;
2) udostępnienie danych osobowych osobom nieupoważnionym;
3) zmiany, kopiowanie lub uszkodzenie danych osobowych dokonane przez osoby nieuprawnione;
4) kradzież nośników informacji zawierających dane osobowe (np. dysków, dyskietek, płyt CD, płyt DVD, wydruków komputerowych).

§ 3

Za okoliczności, które wskazują na naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych, uważa się między innymi:
1) nieuzasadnione korzystanie z zasobów systemu informatycznego lub innego zbioru danych;
2) nieuzasadnione ujawnienie danych osobowych;
3) ujawnienie wirusów komputerowych lub innych programów, które mogą mieć negatywny wpływ na funkcjonowanie systemu informatycznego;
4) wydarzenia obniżające stan bezpieczeństwa systemu informatycznego lub innego zbioru danych (np. awaria zasilania).

§ 4

Osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym lub innym zbiorze danych, która stwierdzi lub podejrzewa naruszenie zabezpieczenia danych zobowiązana jest do:
1) niezwłocznego poinformowania o tym fakcie administratora bezpieczeństwa informacji i swojego bezpośredniego przełożonego,
2) zaprzestania pracy w systemie informatycznym lub innym zbiorze danych do momentu otrzymania od ABI decyzji o możliwości wznowienia pracy.

§ 5

1. ABI po uzyskaniu informacji, o której mowa § 4 zawiadamia o naruszeniu zabezpieczenia danych osobowych ADO Uniwersytetu Warszawskiego i bezpośredniego przełożonego oraz podejmuje działania w celu rozpoznania naruszenia zabezpieczenia danych, a w szczególności ustala, czy miało miejsce naruszenie ochrony danych osobowych, a w sytuacji niepotwierdzenia podejrzeń wydaje decyzję, o której mowa w § 4 ust.1 pkt 2 oraz sporządza i przedstawia w ciągu 14 dni ADO UW raport o podejrzeniu naruszenia ochrony danych osobowych w systemie informatycznym lub innym zbiorze danych.

2. ABI w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych:

1) podejmuje działania służące ograniczeniu szkód wywołanych naruszeniem ochrony danych osobowych;
2) zabezpiecza dane wskazujące na naruszenie zabezpieczenia danych osobowych;
3) ustala okoliczności naruszenia ochrony danych osobowych;
4) analizuje rodzaj, zakres i źródło naruszenia ochrony danych osobowych;
5) podejmuje działania naprawcze;
6) bada przyczyny naruszenia ochrony danych osobowych i podejmuje działania mające na celu wyeliminowanie podobnych zdarzeń zagrażających bezpieczeństwu danych.

§ 6

Administrator bezpieczeństwa informacji, po czynnościach, o których mowa w § 5, sporządza i przedstawia ADO UW raport o stwierdzeniu naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych w ciągu 14 dni od daty jego zaistnienia. Raport zawiera w szczególności następujące dane i informacje:

1) imię i nazwisko, stanowisko osoby, która zgłosiła naruszenie zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze danych;
2) miejsce zatrudnienia osoby, o której mowa w pkt 1;
3) datę i godzinę powiadomienia o naruszeniu;
4) opis podjętych działań mających na celu ustalenie zakresu podejrzewanego naruszenia.
5) opis podjętych działań naprawczych.

§ 7

Administrator bezpieczeństwa informacji jest odpowiedzialny za przechowywanie materiałów, o których mowa § 5, dokumentujących zaistniałe naruszenie oraz podejrzenie naruszenia zabezpieczenia danych w systemie informatycznym lub innym zbiorze danych.