Nr 293/2005

Z A R Z Ą D Z E N I E Nr 293/2005

PREZYDENTA MIASTA RADOMIA

z dnia 26.07.2005 r.

w sprawie: **wprowadzenia “Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Radomiu”.**

Na podstawie § 4 pkt 8 Regulaminu Organizacyjnego Urzdu Miejskiego w Radomiu wprowadzonego Zarzdzeniem Nr 155/2005 z dnia 29 kwietnia 2005 r. z a r z d z a m, co nastpuje:

§ 1.

Wprowadzam “Instrukcj zarzdzania systemem informatycznym sucym do przetwarzania danych osobowych w Urzdzie Miejskim w Radomiu”, która stanowi zacznik do niniejszego zarzdzenia.

§ 2.

Zobowizuj dyrektorów wydziaów oraz kierowników równorzdnych komórek organizacyjnych Urzdu do wykonania zarzdzenia oraz zapoznania z zapisami “Instrukcji…” podlegych im pracowników.

§ 3.

Traci moc Zarzdzenie Nr 355/2003 Prezydenta Miasta Radomia z dnia 27 paŸdziernika 2003 r. w sprawie wprowadzenia “Instrukcji uytkowania programów komputerowych oraz baz danych Urzdu Miejskiego w Radomiu”.

§ 4.

Zarzdzenie wchodzi w ycie z dniem podpisania.

INSTRUKCJA ZARZDZANIA SYSTEMEM INFORMATYCZNYM SUCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZDZIE MIEJSKIM w RADOMIU

Data wydania dokumentu: 26.07.2005 r.

Zastępuje: Zarządzenie Prezydenta Miasta Radomia 355/2003 z dn. 27.10.2003 r.

z dnia 29 sierpnia 1997 r. o *ochronie danych osobowych* § 3 ustęp 1 i § 5 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 101 poz. 926 z 2002 r., z późniejszymi zmianami, Dz. U. Nr 100, poz. 1024)

I. WSTĘP

Program komputerowy zgodnie z ustawą *o prawie autorskim i prawach pokrewnych z* dnia 4 lutego 1994 r. jest przedmiotem prawa autorskiego i podlega ochronie. Ochrona obejmuje wszystkie formy wyrażania programu komputerowego, w tym wszystkie formy, wytwórczej i użytkowej.

Zgodnie z ustawą z dnia 29 sierpnia 1997 r. o *ochronie danych osobowych* dokumentacji projektowej każdy ma prawo do ochrony dotyczących go danych osobowych.

W związku z powyższym ustala się sposób postępowania z danymi, programami, systemami informatycznymi oraz ze stanowiskiem komputerowym:

Ilekroć w instrukcji jest mowa o

Administratorze Danych - rozumie się przez to Prezydenta Miasta Radomia.

Administratorze Bezpieczeństwa Informacji - należy przez to rozumieć pracownika w Biurze Ochrony wyznaczonego przez Prezydenta Miasta do nadzorowania przestrzegania wymagań w zakresie ochrony danych osobowych wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.

Administratorze Systemu Informatycznego - należy przez to rozumieć pracownika lub pracowników Referatu ds. Informatyki odpowiedzialnych za funkcjonowanie systemu informatycznego Urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie.

Przetwarzaniu danych osobowych - naley przez to rozumie jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostpnianie i usuwanie.

Urzdzie - naley przez to rozumie Urzd Miejski w Radomiu.

Systemach informatycznych - naley przez to rozumie systemy suce do przetwarzania danych osobowych.

Uytkowniku (-ach) - naley przez to rozumie pracownika (-ów) Urzdu Miejskiego oraz staystów posiadajcych uprawnienia do przetwarzania danych osobowych.

Uwierzytelnieniu - naley przez to rozumie identyfikacj uytkownika wraz z hasem potwierdzajca jego uprawnienia.

1. **III.**

3.

4. 1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

5. - Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.),

6. - Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. 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)

7. - Zarządzeniem Prezydenta Nr 293/2005 z dnia 26.07.2005 r. wprowadzającym Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych

8. 2. Każdy kierownik komórki organizacyjnej, w której są przetwarzane dane osobowe ma obowiązek prowadzenia **rejestru pracowników tej komórki posiadających upoważnienia dostępu do zbiorów osobowych i nadanych uprawnień do przetwarzania innych danych.**

9. Do obsługi systemu komputerowego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, użytkownik może być dopuszczony wyłącznie posiadając upoważnienie wydane przez administratora danych lub upoważnioną przez niego osobę.

10. 4. Do obsugi systemu komputerowego oraz urzdze wchodzcych w jego skad, sucych do przetwarzania danych innych ni osobowe, uytkownik moe by dopuszczony za zgod przeoonego (kierownika komórki organizacyjnej).

ADMINISTRATOR DANYCH OSOBOWYCH:

Dane osobowe udostępniać może wyłącznie administrator danych lub upoważniona przez niego osoba.

Dane osobowe można udostępniać wyłącznie na pisemny, umotywowany wniosek (powinien zawierać

1. informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie) osobom lub podmiotom uprawnionym do ich otrzymywania na mocy przepisów prawa.

Innym osobom lub podmiotom niż wymienione w pkt. 2 dane osobowe mogą być udostępnione, jeżeli

1. w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego

1. zostay udostpnione.

Administrator Danych może odmówić udostępnienia danych, jeżeli zachodzi jakakolwiek sprzeczność

1. z ustawą o ochronie danych osobowych (art. 30 ustawy o ochronie danych osobowych).

Wszystkie wydawane wydruki są ewidencjonowane przez osobę upoważnioną przez administratora

1. danych osobowych.

2. **Administrator Danych Osobowych zapewnia osobie, której dane dotyczą możliwość uzyskania informacji o odbiorcach, którym dane osobowe zostały udostępnione zgodnie z artykułem 7 punkt 6 Ustawy o Ochronie Danych Osobowych. Obowiązek ten realizuje poprzez Administratora Systemu Informatycznego i kierowników komórek organizacyjnych Urzędu.**

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI:

1.

2. **2.** Nadzoruje i kontroluje realizację i stosowanie polityki bezpieczeństwa oraz zabezpieczenia danych przetwarzanych zarówno tradycyjnie jak i danych przetwarzanych w systemach informatycznych.

3. **3.** Opracowuje instrukcję określającą sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

4. **4.** Nadzoruje i kontroluje realizację zapisów instrukcji a w szczególności:

5. - zastosowanych rozwiązań technicznych,

6. - procedur eksploatacji,

7. - zasad użytkowania,

8. zastosowanych w celu zabezpieczenia danych osobowych w Urzędzie Miejskim w Radomiu przed ich nieuprawnionym przetwarzaniem.

9. **5.** Identyfikuje i analizuje zagrożenia ujawnienia danych oraz opracowuje sposoby ochrony danych osobowych.

10. **6.** Prowadzi szkolenie pracowników w zakresie realizacji polityki bezpieczeństwa poprzez dostarczanie wiedzy o ochronie informacji.

11. **7.** Kontroluje prawidłowość wykonywanych zadań przez Administratora Systemu Informatycznego.

Prowadzi rejestr umów powierzenia na przetwarzanie danych osobowych innym podmiotom.

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

1. Użytkownicy systemu, programu są niezwłocznie rejestrowani i wyrejestrowywani przez administratora systemu informatycznego, gdy uzyskują lub tracą prawo do dostępu do systemu, programu.

2. Po wyrejestrowaniu użytkownika jego identyfikator dostępu do systemu nie może być przydzielany innej osobie.

3. Identyfikator oraz pierwsze hasło jest przydzielane użytkownikowi przez administratora systemu informatycznego.

4. prowadzi rejestr użytkowników przetwarzających dane osobowe (odnotowywane jest imię i nazwisko użytkownika, identyfikator oraz pierwsze hasło).

5. Kopie awaryjne są tworzone codziennie, nośnikiem są dyski, tasiemki streamera, co kwartał tworzone są kopie na płytach CD-ROM.

6. Nośniki informacji przechowywane są w pokojach Ref. ds. Informatyki przez okres 2 tygodni o ile sytuacja nie wymaga inaczej; po upływie tego okresu albo są wykorzystywane do ponownej kopii albo ulegają zniszczeniu; kopie awaryjne są okresowo sprawdzane pod kątem ich dalszej przydatności.

7. Monitory ekranowe są usytuowane w taki sposób, że uniemożliwiają odczyt danych przez osoby postronne.

8. Systemy komputerowe są tak skonfigurowane, że po upływie określonego czasu bezczynności wyłączają się.

9. Systemy komputerowe, programy oraz nośniki sprawdzane są na obecność wirusa z częstotliwością l miesiąca (o ile nie zajdzie inna potrzeba).

10. Przeglądy i konserwacja systemów i zbiorów danych przeprowadzane są co miesiąc przez uprawnione do tego osoby pod nadzorem osoby

upoważnionej przez administratora danych.

11. Urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem innemu podmiotowi należy pozbawić ich zawartości; w przypadku likwidacji należy uszkodzić w sposób uniemożliwiający odczytanie danych; naprawę wymienionych urządzeń zawierających dane osobowe, o ile danych nie można usunąć, należy wykonywać pod nadzorem osoby upoważnionej przez administratora danych.

1. **Administrator Systemu Informatycznego zapewnia możliwość sporządzania i wydrukowania raportów zawierających informację wskazaną w § 7 ust. 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r.**

PROCEDURA NADAWANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1. **1.** Kierownik komórki organizacyjnej, w ciągu 7 dni od chwili zatrudnienia pracownika, występuje do Administratora Danych z wnioskiem o wydanie upoważnienia do dostępu do zbioru dla pracownika. Wniosek powinien zawierać: nazwisko i imię, zajmowane stanowisko, nazwę zbioru, zakres upoważnienia oraz termin obowiązywania.

2. **2.** Na podstawie zaakceptowanego wniosku Biuro Ochrony przygotowuje stosowne upoważnienie, nadając mu numer rejestrowy i identyfikator do zbioru w porozumieniu z Administratorem Systemu Informatycznego

3. **3.** Na podstawie wydanego upoważnienia administrator systemu informatycznego udziela dostępu do zbioru.

4. **4.** Kierownik komórki organizacyjnej, w ciągu 7 dni od zwolnienia lub przeniesienia pracownika do innej komórki organizacyjnej, jest zobowiązany złożyć wniosek do administratora danych o unieważnienie upoważnienia temu pracownikowi.

5. **5.** Centralna ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona w Biurze Ochrony Urzędu.

PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA INNYCH DANYCH

Dla pracowników posiadających identyfikator i hasło do sieci komputerowej - Kierownik komórki organizacyjnej zgłasza Administratorowi Systemu Informatycznego, że wyraża zgodę na udzielenie dostępu do zbioru.

Dla pracowników nie posiadających identyfikatora i hasła do sieci komputerowej - Kierownik komórki organizacyjnej występuje do Administratora Systemu Informatycznego, z wnioskiem o udzielenie dostępu do zbioru. Wniosek powinien zawierać: nazwisko i imię, zajmowane stanowisko, nazwę zbioru, zakres uprawnień.

Kierownik komórki organizacyjnej, w ciągu 7 dni od zwolnienia lub przeniesienia pracownika do innej komórki organizacyjnej, jest zobowiązany złożyć wniosek do Administratora Systemu Informatycznego o unieważnienie dostępu do zbioru temu

pracownikowi.

IV.

W systemie informatycznym stosuje się uwierzytelnianie w zakresie:

1. - dostępu do sieci lokalnej

2. - dostępu do aplikacji

3. - dostępu do sieci publicznej

4. uzależnione od stopnia bezpieczeństwa.

W Urzędzie Miejskim w Radomiu stosowane są poziomy bezpieczeństwa w systemach informatycznych na poziomach:

- podstawowy

- podwyzszony

- wysoki

Poziom bezpieczeństwa **podstawowy** obejmuje zabezpieczenie systemów informatycznych

przed dostepem osób nieuprawnionych podczas nieobecności osób upoważnionych do przetwarzania danych. Osoby nieuprawnione mogą przebywać w obszare przetwarzania danych za zgodą administratora danych lub w obecności osób upoważnionych do przetwarzania danych osobowych. Bezpośredni dostęp do danych zapewniony jest po podaniu identyfikatora i właściwego hasła. Hasło jest zmieniane z częstotliwością nie rzadszą niż 28 dni, składa się, co najmniej, z 6 znaków, nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innym osobom. Użytkownik zamyka system, aplikację, program po zakończeniu pracy, stanowisko komputerowe z uruchomionym systemem, aplikacją, programem nie pozostaje bez kontroli pracującego na nim użytkownika.

Poziom bezpieczeństwa **podwyższony** obejmuje stosowanie identyfikatorów i haseł. Hasła są zmieniane z częstotliwością nie rzadszą niż 28 dni, składają się, co najmniej, z 8 znaków, zawierają małe i duże litery oraz cyfry lub znaki specjalne, nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innym osobom. Użytkownik zamyka system, aplikację, program po zakończeniu pracy, stanowisko komputerowe z uruchomionym systemem, aplikacją, programem nie pozostaje bez kontroli pracującego na nim użytkownika.

Poziom bezpieczeństwa **wysoki** obejmuje zabezpieczenie systemów informatycznych poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostepem

oraz stosowanie metod kryptograficznych. Bezpośredni dostęp do danych zapewniony jest po podaniu identyfikatora i właściwego hasła. Hasło jest zmieniane z częstotliwością nie rzadszą niż 28 dni, składa się, co najmniej, z 8 znaków, zawiera małe i duże litery oraz cyfry lub znaki specjalne, oraz nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innym osobom. Użytkownik zamyka system, aplikację, program po zakończeniu pracy, stanowisko komputerowe z uruchomionym systemem, aplikacją, programem nie pozostaje bez kontroli pracującego na nim użytkownika.

UYTKOWNIK

Do obsługi systemu komputerowego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, są dopuszczeni wyłącznie pracownicy (stażyści) posiadający upoważnienie wydane przez administratora danych lub upoważnioną przez niego osobę.

Do obsługi systemu komputerowego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych innych niż osobowe, użytkownik jest dopuszczony za zgodą przełożonego (kierownika komórki organizacyjnej).

Bezpośredni dostęp do danych użytkownik ma dopiero po podaniu identyfikatora i właściwego hasła,

Użytkownik zmienia hasło z częstotliwością nie rzadszą niż 28 dni, hasło musi składać się z, w zależności od poziomu bezpieczeństwa, co najmniej 6 do 8 znaków, nie jest zapisywane w miejscu dostępnym dla osób nieuprawnionych i stosowaniu

zabezpieczeń kryptograficznych.

Użytkownik zamyka system, aplikację, program po zakończeniu pracy, stanowisko komputerowe z uruchomionym systemem, programem nie może pozostać bez kontroli pracującego na nim użytkownika,

Osoby dopuszczone do obsługi programu komputerowego obowiązane są do zachowania tajemnicy co do sposobu dostępu do danych osobowych i ich merytorycznej treści a także sposobu zabezpieczeń, obowiązek ten istnieje również po ustaniu zatrudnienia.

Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, zaś po upływie czasu ich przydatności powinny być niszczone w taki sposób by uniemożliwić odczytanie danych.

Kierownicy komórek organizacyjnych oraz wszyscy pracownicy Urzędu są zobowiązani do przestrzegania niniejszej instrukcji.

Osoby fizyczne oraz inne podmioty wykonujące umowy na rzecz gminy powinny posiadać aktualne upoważnienia wydane przez **Administratora Danych Osobowych** zezwalające na korzystanie ze zbiorów danych.

Na kierowniku komórki organizacyjnej spoczywa obowiązek przygotowania umów powierzenia zbioru danych oraz zarejestrowanie ich w rejestrze prowadzonym przez

Administratora Bezpieczeństwa Informacji.

Użytkownik ma obowiązek powiadamiać administratora bezpieczeństwa informacji o sytuacjach nadzwyczajnych, o wszelkiego rodzaju różnicach w funkcjonowaniu programu, systemu i tylko w porozumieniu z wymienioną osobą może zostać wezwany do konsultacji autor programu lub przedstawiciel autora (firmy, od której zostało oprogramowanie zakupione).

ZABRANIA SI:

Udostępniania identyfikatora, hasła, stanowiska roboczego oraz istniejących na nim danych (w postaci pisanej jak i elektronicznej) osobom nieupoważnionym.

Ingerowania w bazę danych narzędziami innymi niż przeznaczona do tego aplikacja.

Wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez administratora danych.

Samowolnego instalowania i używania programów komputerowych (posiadających lub

nie posiadających licencji).

Trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie.

Niezgodnym z licencją publicznego udostępniania programów komputerowych lub ich kopii dla osób postronnych.

Przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko.

Tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w programie komputerowym.

Używania oprogramowania, które posiada sfałszowane znaki firmowe lub nie posiada w ogóle znaków firmowych, etykiet, oryginalnych nośników, dokumentacji łącznie z elektroniczną.

Udostępniania osobom postronnym (nie bedącym pracowników Urzędu) programów komputerowych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu.

Wykorzystywania oprogramowania lub materiałów ściągniętych z Internetu do rozprowadzania bez licencji lub wyraźnego upoważnienia autora.

Używania nośników udostępnianych przez osoby postronne (nie bedącym pracowników

Urzędu) i podejrzanych o zainfekowanie wirusem. W razie podejrzenia o zainfekowanie wirusem nośnika danych (dyskietki lub dysku twardego) użytkownik ma obowiązek niezwłocznie poinformować o tym Administratora Systemu Informatycznego.

Używania oprogramowania w większym zakresie niż pozwala na to umowa licencyjna.

Używania komputerów przenośnych (w tym między innymi: laptop, notebook, pda) lub dysków i innych elektronicznych nośników informacji (w tym między innymi: do flash drive, pen drive) do przetwarzania danych osobowych.

V. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Na fakt naruszenia zabezpieczeń systemu informatycznego mogą wskazywać:

stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem).

wszelkiego rodzaju różnice w funkcjonowaniu systemu, programu (np. komunikaty

informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach) .

różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych) .

jakości komunikacji w sieci telekomunikacyjnej (gwałtowne opóźnienia lub przyśpieszenia wykonywanych czynności) .

inne sytuacje nadzwyczajne.

W przypadku, stwierdzenia naruszenia zabezpieczeń systemu informatycznego należy niezwłocznie powiadomić Administratora Danych lub inną upoważnioną przez niego osobę oraz Administratora Bezpieczeństwa Informacji.

Używanie nielegalnych programów komputerowych bez zezwolenia właściciela praw autorskich jest zabronione i podlega sankcjom cywilnym i karnym (odpowiedzialność cywilną i karną ponosi zarówno pracownik korzystający z nielegalnego oprogramowania jak i jego przełożeni).

Przetwarzanie i udostępnianie danych osobowych przez osoby nieuprawnione oraz modyfikacja, uszkodzenie lub zniszczenie podlega sankcjom cywilnym i karnym (także

wtedy, gdy sprawca działa nieumyślnie).

Pliki do pobrania

Zarz293.doc
Z A R Z Ą D Z E N I E Nr 293/2005 PREZYDENTA MIASTA RADOMIA z dnia 26.07.2005 r. w sprawie: wprowadzenia “Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Radomiu”.
doc, 37.5 KB,

Metadane

Data publikacji : 27.07.2005

Obowiązuje od : 27.07.2005

Rejestr zmian

Podmiot udostępniający informację:
Urząd Miejski w Radomiu

Osoba wytwarzająca/odpowiadająca za informację:

Osoba udostępniająca informację:
Ryszarda Kitowska

Następny Strona