ZARZĄDZENIE NR 56/2009
STAROSTY TUCHOLSKIEGO
z dnia 4 grudnia 2009.

w sprawie wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi"

Na podstawie Art.36 ust 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity opublikowany w Dz.U. 2002 r. nr 101 poz.926 ze zm.) w związku z §3 i §4 ust. 1 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)

zarządzam, co następuje:

§ 1. 1. W celu uregulowania spraw związanych z ochroną danych osobowych zgodnie z wymaganiami wynikającymi z obowiązujących w tym zakresie przepisów wprowadzam „Politykę bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi", stanowiącą załącznik do niniejszego zarządzenia.

2. Dokument, o którym mowa w § 1 ust. 1, obowiązuje wszystkich pracowników zatrudnionych w Starostwie Powiatowym przy przetwarzaniu tych danych.
3. Postanowienia polityki bezpieczeństwa, w których jest mowa o „pracownikach": stosuje się odpowiednio także do innych osób urzędowo upoważnionych przez Starostę do takiego dostępu do zbiorów danych osobowych, który umożliwia dokładniejsze zapoznanie się z tymi danymi, w szczególności do osób wdrażających i konserwujących systemy przetwarzania danych osobowych, osób odbywających w Starostwie aplikację lub praktykę zawodową albo szkolenie, studentów zbierających materiały do prac dyplomowych itp.

§ 2. Traci moc Zarządzenie Starosty tucholskiego Nr 3/2005 z dnia 24 stycznia 2005 r. w sprawie wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi"

§ 3. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

STAROSTA TUCHOLSKI
Piotr Mowiński

Załącznik do Zarządzenia Nr 56/2009
Starosty Tucholskiego
z dnia 4 grudnia 2009 r.

Polityka bezpieczeństwa przetwarzania danych osobowych

w Starostwie Powiatowym w Tucholi

Opracował : Administrator Bezpieczeństwa Informacji

Spis treści:

Wprowadzenie

Niniejszy dokument opisuje ogólne reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych, rejestrach ręcznych w Starostwie Powiatowym w Tucholi.
Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych oraz pracowników przetwarzających dane w systemie ręcznym.
Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Dokument „Polityka bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi" zwany dalej „polityką bezpieczeństwa", wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych przeznaczony jest dla osób zatrudnionych przy przetwarzaniu danych.

Potrzeba jego opracowania wynika § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (dz. U. Nr 100, poz. 1024).

1. Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:
   a. stwierdzono naruszenie systemu informatycznego, w którym są przetwarzane dane osobowe,
   b. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Starostwa Powiatowego Tucholi.
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w Starostwie.
4. Administrator danych, którym jest Starosta, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych osobowych, zwanego dalej Administratorem Bezpieczeństwa oraz osobę upoważnioną do zastępowania Administratora Bezpieczeństwa.
5. Administrator Bezpieczeństwa realizuje zadania w zakresie ochrony danych, w szczególności:
   a. opracowuje ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych i w zbiorach ręcznych urzędu,
   b. podejmowania stosownych działań zgodnie z niniejszą polityką bezpieczeństwa w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych osobowych znajdujących się w systemach informatycznych i pozostałych zbiorach,
   c. niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,

d. nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.
7. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

Niniejszy dokument jest zgodny z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002, Nr 101, poz. 926 z późn. zm.).

Rozdział 1
Opis zdarzeń naruszających ochronę danych osobowych

1. Podział zagrożeń:
   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) ich występowanie może doprowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   3) zagrożenia świadome, zamierzone i celowe – najpoważniejsze zagrożenia naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy).
   Zagrożenia te możemy podzielić na:
   a. nieupoważniony dostęp do systemu z zewnątrz (włamanie do systemu),
   b. nieupoważniony dostęp do systemu z jego wnętrza,
   c. nieuprawniony przekaz danych,
   d. pogorszenie jakości sprzętu i oprogramowania,
   e. bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   a. sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby jak np. wybuch gazu, pożar zalanie, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   b. niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od uderzeń przemysłowych,
   c. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
   d. pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   e. jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie,

f. naruszenie lub próba naruszenia integralności systemu lub bazy danych w systemie,
g. stwierdzone próby lub modyfikacje danych lub zmiany w strukturze danych bez odpowiedniego upoważnienia,
h. niedopuszczalna manipulacja danymi osobowymi w systemie,
i. ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,
j. praca w systemie lub w jego sieci komputerowej wskazująca nieprzypadkowe odstępstwa od założonego rytmu pracy, wskazująca na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.,
k. ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki",
l. podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony, skasowanie lub skopiowanie danych osobowych,
m. rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział 2
Zabezpieczenie danych osobowych

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych i ręcznych Starostwa Powiatowego w Tucholi jest Starosta.
2. Administrator danych osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Starostwa, a w szczególności:
   a. zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   b. zapobiegać przed zabraniem danych przez osobę nieupoważnioną,
   c. zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
3. Do zastosowanych środków technicznych należy:
   a. przetwarzanie danych osobowych w wyznaczonych pomieszczeniach położonych w strefie administracyjnej,
   b. zabezpieczenie wejścia do pomieszczeń, o których mowa w punkcie **a**,
   c. szczegółowe zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   d. wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

4. Do zastosowanych środków organizacyjnych należą przede wszystkim zasady:
   a. zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych,
   b. przeszkolenie osób, o których mowa w punkcie **a**, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
   c. kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.
5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka Bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy czynności osób zatrudnionych przy przetwarzaniu danych osobowych w systemie.
6. Wykaz pomieszczeń, w których przetwarzane są dane osobowe oraz opis systemów informatycznych i ręcznych Starostwa Powiatowego w Tucholi i ich zabezpieczeń zawiera załącznik nr 1 do niniejszego dokumentu.

Rozdział 3
Kontrola przestrzegania zasad zabezpieczania danych osobowych

1. Administrator danych lub osoba przez niego wyznaczona, którą jest Administrator Bezpieczeństwa sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. Administrator Bezpieczeństwa sporządza roczne plany kontroli zatwierdzone przez Starostę i zgodnie z nimi przeprowadza kontrole oraz dokonuje rocznych ocen stanu bezpieczeństwa danych osobowych.
3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2 Administrator Bezpieczeństwa sporządza sprawozdania roczne i przedstawia Administratorowi danych.

Rozdział 4
Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia:
   a. zabezpieczenia systemu informatycznego,
   b. technicznego stanu urządzeń,
   c. zawartości zbioru danych osobowych, także rejestrów ręcznych,
   d. ujawnienia metody pracy lub sposobu działania programu,
   e. jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   f. innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (pożar, zalanie).

Osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana powiadomić o tym fakcie Administratora Bezpieczeństwa!

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:
   a. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców,
   b. rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c. zaniechać - o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   d. podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
   e. podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   f. zastosować się do innych instrukcji i regulaminów, jeśli odnoszą się one do zaistniałego przypadku,
   g. udokumentować wstępnie zaistniałe naruszenie,
   h. nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.
4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administrator Bezpieczeństwa lub osoba go zastępująca:
   a. zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy urzędu,
   b. może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   c. rozważa celowość i potrzebę powiadamiania o zaistniałym fakcie Administratora danych,
   d. nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba ze specjalistami spoza urzędu.
5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 2, który powinien zawierać w szczególności:
   a. wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   b. określenie czasu, miejsca naruszenia i rodzaju naruszenia,
   c. wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   d. wstępną ocenę wystąpienia naruszenia,
   e. ocenę przeprowadzonego postępowania wyjaśniającego.
6. Raport, o którym mowa w ust. 5 Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi danych, a w przypadku jego nieobecności osobie uprawnionej.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej zespołowej analizy prowadzonej przez Kierownictwo urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Informacji niejawnych.
9. Analiza, o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5
Postanowienia końcowe

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonym zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 3 do niniejszego dokumentu.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002, Nr 101, poz. 926), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr. 100, poz 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych (Dz. U. Nr 100, poz. 1023).
6. Niniejsza „Polityka bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi" wchodzi w życie z dniem podpisania jej przez Starostę.