Zarządzenie Nr 16/ 99
Starosty Wyszkowskiego
z dnia 20 października 1999r.

w sprawie ochrony danych w Starostwie Powiatowym w Wyszkowie.

Na podstawie art. 34 i art. 35 ustawy z dnia 5 czerwca 1998r. o samorządzie powiatowym (Dz. U Nr 91 poz. 578 z późn. zm), przepisów rozdziału 5 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. Nr 133 poz. 883) oraz § 11 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetworzenia danych osobowych (Dz. U. Nr 80 poz. 521) **zarządzam,** co następuje:

§ 1.

W celu zapewnienia należytego bezpieczeństwa danych osobowych przetwarzanych w Starostwie Powiatowym w Wyszkowie, szczególnie w przypadku, jeżeli przetwarzane są w systemach informatycznych, wprowadza się:

1. Zasady postępowania przy przetwarzaniu danych osobowych w Starostwie Powiatowym w Wyszkowie (załącznik nr 1).
2. Instrukcje zarządzania systemem informatycznym służącym do przetworzenia danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji oraz postępowania w sytuacji naruszenia ochrony danych osobowych (załącznik nr 2).

§ 2.

Zobowiązuje wszystkich pracowników Starostwa mających dostęp do danych osobowych zawartych w zbiorach Starostwa do ścisłego przestrzegania niniejszym zarządzeniem instrukcji.

§ 3.

Zobowiązuję wszystkich pracowników mających dostęp do danych osobowych do złożenia oświadczenia o zachowaniu tajemnicy treści danych osobowych, z którymi w toku pracy zapoznają się.

§ 4.

Zobowiązuje inspektora ds. pracowniczych do przechowywania oświadczeń w teczkach akt osobowych.

§ 5.

Za wykonanie zarządzenia czynię odpowiedzialnym Sekretarza Powiatu.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Stanisław Jastrzębski

Załącznik nr 1
do Zarządzenia Nr 16/99
Starostwa Wyszkowskiego
z dnia 20 października 1999r.

Zasady postępowania przy przetwarzaniu danych osobowych w Starostwie Powiatowym w Wyszkowie.

§ 1.

Przetwarzanie danych osobowych w Starostwie Powiatowym w Wyszkowie jest prowadzone na zasadach określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883) przepisach wykonawczych do ustawy oraz na podstawie "Zasad postępowania przy przetwarzaniu danych osobowych w Starostwie Powiatowym w Wyszkowie, zwanych dalej "zasadami".

§ 2.

Przez użyte w zasadach określenia należy rozumieć:

1. dane osobowe - każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby,
2. zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
3. przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych takie, jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza te, które wykonuje się w systemach informatycznych,

4. administrator danych osobowych - Starosta Wyszkowski,

5. administrator bezpieczeństwa informacji - osoba wyznaczona przez administratora danych osobowych odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

6. naczelnik - naczelnik wydziału Starostwa Powiatowego w Wyszkowie

7. użytkownik - osoba przetwarzająca dane.

§ 3.

Administrator danych osobowych decyduje o celach i środkach przetwarzania danych osobowych.

§ 4.

1. Administrator danych osobowych jest zobowiązany do:

1) czuwania nad tym, by będące w jego posiadaniu dane osobowe były przetwarzane zgodnie z prawem,
2) zastosowania niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych w Starostwie danych osobowych,
3) sprawowania kontroli nad bezpieczeństwem oraz sposobem przetwarzania danych,
4) rejestracji w Głównym Inspektoracie Ochrony Danych Osobowych zbiorów danych przed przystąpieniem do ich przetwarzania.

2. Administrator bezpieczeństwa informacji jest zobowiązany do:

1) wprowadzenia w życie i kontroli właściwego przestrzegania "Instrukcji i zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji",

2) reagowania na wszelkie przesłanki wskazujące na możliwość naruszenia tajemnicy danych osobowych,

3) podjęcia natychmiastowych działań na rzecz ochrony danych w przypadku naruszenia ustawy,

4) prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych,

5) opracowania i wdrożenia programu szkolenia w zakresie zabezpieczeń systemu informatycznego,

6) sygnalizowania niezgodności przepisów oraz aktów wewnętrznych Starostwa z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawiania stosownych projektów zmian w celu dostosowania ich do regulacji ustawowych.

3. Naczelnicy Wydziałów Starostwa są zobowiązani do:

1) współdziałania z administratorem bezpieczeństwa informacji w zakresie przestrzegania instrukcji, o której mowa w ust. 2 pkt. 1

2) opracowania dla każdej osoby zatrudnionej przy przetwarzaniu danych osobowych zakresu czynności z uwzględnieniem stopnia dostępu do danych osobowych oraz przewidzianej odpowiedzialności za naruszenie tajemnicy danych odpowiednio do zakresu obowiązków,

3) sprawowania nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający należytą ochroną danych osobowych,

4) zwracania się do administratora danych o rozstrzygnięcie w przypadku istotnych wątpliwości w stosowaniu przepisów prawnych z zakresu ochrony danych osobowych,

5) niezwłocznego zawiadomienia administratora danych osobowych o konieczności utworzenia nowego zbioru danych osobowych, wymagającego rejestracji.

4. Pracownik upoważniony do przetwarzania danych osobowych, przez administratora danych jest zobowiązany do:

1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,

2) stosowania określonych przez administratora danych, procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,

3) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania. danych w celu ochrony interesów osób, których te dane dotyczą,

4) podporządkowania się poleceniom administratora bezpieczeństwa informacji oraz właściwego naczelnika, w zakresie ochrony danych.

§ 5.

1. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez administratora danych osobowych. Wzór upoważnienia stanowi załącznik nr 1 do niniejszych zasad.
2 Bezpośredni nadzór nad przetwarzaniem danych osobowych w działach Starostwa sprawują naczelnicy tych wydziałów. Wzór upoważnienia określającego zakres odpowiedzialności stanowi załącznik nr 2.
3. Pracownik, któremu. administrator danych osobowych udzieli upoważnienia, o którym mowa w ust. 2 jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi załącznik nr 4.

4. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzanych danych, dyrektor jest zobowiązany bezzwłocznie skierować wniosek do administratora danych osobowych o wydanie lub cofnięcie upoważnienia. W przypadku samodzielnych stanowisk pracy cofnięcia lub wydania upoważnienia dokonuje administrator danych bezpośrednio. Wzór pisma o cofnięciu upoważnienia stanowi załącznik nr 3.
5. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.

§ 6.

Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.

§ 7.

Przetwarzanie danych osobowych sprzeczne z przepisami ustawy o ochronie danych osobowych może stanowić ciężkie naruszenie obowiązków pracowniczych.

STAROSTA
Stanisław Jastrzębski

Załącznik nr 2
do Zarządzenia Nr 16/99
Starosty Wyszkowskiego
z dnia 20 października 1999r.

INSTRUKCJA

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji oraz postępowania w sytuacji naruszenia ochrony danych osobowych

§ 1.

POSTANOWIENIA OGÓLNE

1. Instrukcja określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie ze szczególnym uwzględnieniem wymogów bezpieczeństwa i ochrony danych osobowych zawartych w systemie informatycznym, kartotekach, księgach, wykazach i innych zbiorach ewidencyjnych. .

2. Przez użyte w instrukcji określenia należy rozumieć:

1) dane osobowe - wszelkie informacje dotyczące osoby fizycznej, pozwalające na określenia tożsamości tej osoby,
2) administrator danych osobowych - Starosta
3) administrator bezpieczeństwa informacji - osoba wyznaczona przez administratora

danych osobowych odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

4) użytkownik - osoba przetwarzająca dane.

§ 2.

PRZETWARZANIE DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych, czyli wszelkie operacje wykonywane na danych zarówno w systemach informatycznych, jak i metodami tradycyjnymi tj. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie powinno być dokonywane zgodnie z prawem i adekwatne w stosunku do celów, w jakich są przetwarzane
2. Dla każdej osoby, której dane są przetwarzane, system powinien zapewniać odnotowanie:

1) daty pierwszego wprowadzenia danych tej osoby,
2) źródła pochodzenia danych, jeśli dane pochodzić mogą z różnych źródeł,
3) identyfikatora użytkownika wprowadzającego dane,
4) informacji komu, kiedy i w jakim zakresie dane zostały udostępnione, jeśli przewidziane jest udostępnianie danych innym podmiotom, chyba, ze dane te traktuje się jako dane powszechnie dostępne,
5) sprzeciwów, o których mowa w art. 32 ust 1 pkt. 7 i 8 ustawy o ochronie danych osobowych.

3. Dane osobowe udostępnia się na pisemny umotywowany wniosek skierowany do administratora danych. Wniosek powinien zawierać informacje umo2liwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

4. Administrator danych odmawia udostępnienia danych osobowych ze zbioru gdy mogłoby to spowodować:

1) ujawnienie wiadomości stanowiących tajemnicę państwową,

2) zagrożenie dla obronności kraju lub bezpieczeństwa państwa, życia lub zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego,

3) istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 3.

OCHRONA DOSTĘPU DO DANYCH OSOBOWYCH
W SYSTEMIE INFORMATYCZYM

l. Osobie upoważnionej przez administratora danych osobowych do przetwarzania danych, administrator bezpieczeństwa informacji przydziela identyfikator, który wraz imieniem i nazwiskiem zostaje wpisany do ewidencji prowadzonej przez administratora danych.

2. Identyfikator składa się z symbolu wydziału oraz symbolu pracownika.

3. Identyfikator nie powinien być zmieniany, a po wyrejestrowaniu nie powinien być przydzielony innej osobie.

4. Z każdym identyfikatorem związane jest hasło określane przez użytkownika i

utrzymywane przez niego w tajemnicy. Hasło powinno zawierać co najmniej 5 znaków i być zmieniane nie rzadziej niż co cztery tygodnie.

5. Identyfikator oraz hasło, osoby; która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego.

6. Użytkownik, który zapomniał hasła, zgłasza ten fakt administratorowi bezpieczeństwa informacji, który ma możliwość zmiany hasła i umożliwić wprowadzenie nowego hasła.

7. Podczas rejestracji użytkownika systemu informatycznego ustala się prawa dostępu do aplikacji obsługującej zbiór danych osobowych, zgodnie z zakresem obowiązków pracownika.

8. W celu przystąpienia do pracy użytkownik wprowadza do systemu:

1) swój identyfikator (login name),

2) indywidualne hasło (password).

9. Po zakończeniu pracy użytkownik zamyka dostęp do danych przez zastosowanie funkcji "logout".

§ 4.

OCHRONA URZĄDZEŃ PRZETWARZAJĄCYCH DANE OSOBOWE

1. Urządzenia służące do przetwarzania danych osobowych zasilane energią elektryczną powinny być zabezpieczone przed utratą tych danych w wyniku awarii lub zakłóceń sieci elektrycznej - zasilaniem awaryjnym.

2. Kopie awaryjne powinny być sporządzane codziennie i archiwizowane w systemie gwarantującym posiadanie przynajmniej trzech ostatnich kopii.

3. Kopie awaryjne powinny być tworzone na odpowiednich nośnikach informacji (np. taśmy magnetyczne) i przechowywane w pomieszczeniu innym niż serwer, w kasie pancernej, do której dostęp powinny mieć dwie upoważnione osoby.

4. Ekrany monitorów urządzeń przetwarzających dane, powinny być zaopatrzone w automatyczne wygaszacze ekranów, . włączające ekran po wprowadzeniu przez użytkownika hasła.

5. Monitory stanowisk dostępu do danych osobowych powinny być ustawione tak aby uniemożliwić wgląd w dane osobom nieupoważnionym:

6. Z urządzeń, dysków lub innych nośników informatycznych zawierających dane osobowe, przeznaczonych do likwidacji należy usunąć zapis lub je uszkodzić w sposób uniemożliwiający odczytanie tych danych.

7. Przed naprawą urządzeń, dysków lub usunąć z nich zapis. zawierający dane osobowe. Naprawa tych urządzeń może odbywać się wyłącznie pod nadzorem osoby upoważnionej przez administratora bezpieczeństwa informacji.

8. Jeżeli istnieje konieczność przewożenia dyskietek, powinny być przewożone w zaplombowanych pudełkach, przez osobę upoważnioną przez administratora bezpieczeństwa informacji.

9. System informatyczny powinien być wyposażony w program antywirusowy.

10. Każda dyskietka, która ma być użyta, .powinna być poddana działaniu programu antywirusowego.

11. Przeglądy i konserwacja systemów, komputerowych są dokonywane na podstawie umów zawartych z uprawnionymi podmiotami.

§ 5.

ZABEZPIECZANIE POMIESZCZEŃ I BUDYNKÓW,
W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

1. Wykaz pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe jest przechowywany w szafie pancernej za pośrednictwem administratora bezpieczeństwa informacji.

2. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na czas nieobecności osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostanie się do środka osób niepowołanych.

3. W pomieszczeniach, w których przetwarza się dane osobowe, osoby trzecie mogą przebywać wyłącznie w obecności osób upoważnionych do przetwarzania danych.

81

POSTĘPOWANIE W SYTUACJACH NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

W przypadku gdy stwierdzono naruszenie zabezpieczenia systemu informatycznego lub urządzenia, albo gdy zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą

wskazywać na naruszenie zabezpieczeń danych, każdy pracownik zobowiązany jest do:

1) powstrzymania się od wszelkich działań mogących utrudnić ustalenie kto, kiedy i w jaki sposób naruszył zabezpieczenie tych danych oraz czyje dane osobowe zostały naruszone,

2) zabezpieczenia pomieszczenia do czasu przybycia administratora bezpieczeństwa informacji,

3) niezwłocznego powiadomienia administratora bezpieczeństwa informacji oraz dyrektora wydziału użytkującej sprzęt komputerowy,

4) sporządzenia notatki służbowej opisującej zdarzenie, którą należy przedłożyć administratorowi bezpieczeństwa informacji.

2. Administrator bezpieczeństwa informacji, w przypadku zaistnienia okoliczności wskazanych powyżej, podejmuje niezwłoczne działania uniemożliwiające dalsze naruszenie ochrony danych osobowych, a w szczególności:

1) wymienia hasło użytkownika systemu informatycznego,

2) dokonuje analizy procedur korzystania z urządzenia oraz komunikacji w sieci komputerowej,

3) zabezpiecza przechowywane w urządzeniu dane osobowe,

4) dokonuje przeglądu technicznego urządzenia i oprogramowania,

5) w razie konieczności odłącza urządzenie od sieci komputerowej.

STAROSTA
Stanisław Jastrzębski

Załącznik nr 1
do Zasad postępowania przy
przetwarzaniu danych osobowych
w Starostwie Powiatowym
w Wyszkowie

UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. nr 133, poz. 883)

upoważniam

Pana/ Panią .....

zatrudnionego/ zatrudnionej w Starostwie Powiatowym w na stanowisku

.....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych

Wyszków, dnia .....

Zobowiązuję:

1. do zastosowania niezbędnych środków technicznych i organizacyjnych określonych w przepisach powszechnie obowiązujących, w celu zapewnienia ochrony przetwarzania danych osobowych w podległym referacie, wydziale, stanowisku. *
2. do kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie.

Wyszków, dnia .....

* Niepotrzebne skreślić

Załącznik nr 2
do Zasad postępowania przy
przetwarzaniu danych osobowych
w Starostwie Powiatowym
w Wyszkowie

UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. nr 133, poz. 883)

upoważniam

Pana/ Panią .....

.....

(stanowisko służbowe)

do przetwarzania danych osobowych, gromadzonych w związku z realizacją przydzielonych obowiązków pracowniczych.

95

Załącznik nr 3
do Zasad postępowania przy
przetwarzaniu danych osobowych
w Starostwie Powiatowym
w Wyszkowie

WYCOFANIE UPOWAŻNIENIA

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o· ochronie danych osobowych (Dz. U. nr 133, poz. 883)
W związku z:

.....

.....

.....

cofam upoważnienie

Panu/Pani.....
zatrudnionemu/ zatrudnionej w Starostwie Powiatowym w Wyszkowie
na stanowisku.....
do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

Wyszków, dnia .....

Załącznik nr 4
do Zasad postępowania przy
przetwarzaniu danych osobowych
w Starostwie Powiatowym
w Wyszkowie

OŚWIADCZENIE

Oświadczam, że zapozanałem/ zapoznałam się z treścią ustawy z dnia 29 sierpnia 1997 roku o ochronie danych. osobowych (Dz. U. nr 13 3, poz. 8 83) oraz Zarządzeniem Starosty Wyszkowskiego z dnia 20 października 1999 roku wraz z załącznikami i zobowiązuję się do przestrzegania tajemnicy. danych osobowych, z którymi mam bezpośredni kontakt w trakcie, jak i po ustaniu zatrudnienia w Starostwie Powiatowym w Wyszkowie, a w szczególności:

- zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których one dotyczą,

- zabezpieczenia danych przed ich udostępnieniem osobom nie upoważnionym.

....

(data) (czytelny podpis pracownika)