ZARZĄDZENIE WEWNĘTRZNE NR 05/10
BURMISTRZA SOKÓŁKI

z dnia 15 marca 2010 r.

W sprawie ochrony danych osobowych

Na podstawie art. 36 ust. 1 pkt. 2 i ust. 3 Ustawy o ochronie danych osobowych (tekst jednolity Dz. U. Z 2002 r., nr 101, poz. 926 z późniejszymi zmianami), oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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. z 2004 r., nr 100, poz. 1024), zarządzam co następuje:

§ 1. W celu właściwego zabezpieczenia i ochrony danych osobowych w Urzędzie Miejskim w Sokółce wprowadzam:

1) „Politykę bezpieczeństwa" stanowiącą załącznik nr 1 do zarządzenia.
2) „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącą załącznik nr 2 do zarządzenia.

§ 2. Traci moc zarządzenie Nr 11/99 Burmistrza Miasta i Gminy Sokółka z dnia 18 października 1999 r. w sprawie ochrony danych osobowych.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Stanisław Małachwiej

RADCA PRAWNY
mgr Danuta Kamieniuk
dn. 15.03.2010r.

15.03.2010

2010-03-15 14:50:00

Załącznik nr 1
Do Zarządzenie wewnętrznego Nr 05/10
Burmistrza Sokółki
z dnia 15.03.2010 r.

Polityka bezpieczeństwa

Spis treści

1 Definicje

a) 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.
b) Administrator danych osobowych - zadania administratora danych osobowych wykonuje Burmistrz Sokółki.
c) Administrator bezpieczeństwa informacji - osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych we wskazanych systemach informatycznych.
d) Administrator systemu informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w Urzędzie Miejskim w Sokółce.
e) System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
f) Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
g) Bezpieczeństwo systemu informatycznego - wdrożenie przez administratora danych

osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.

h) Przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
i) Osoba upoważniona - osoba posiadająca upoważnienie wydane przez administratora danych osobowych i dopuszczona jako użytkownik do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.
j) Użytkownik systemu - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
k) Osoba uprawniona - osoba posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności.
l) Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
m) Rozporządzenie - rozporządzenie 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.

2 Zasady ogólne

a) Ochrona danych osobowych przetwarzanych w Urzędzie Miejskim w Sokółce obowiązuje wszystkie osoby, które mają dostęp do informacji przetwarzanych w urzędzie, bez względu na zajmowane stanowisko oraz miejsce wykonywania pracy, jak również charakter stosunku pracy. Ochroną objęte są również dane pozyskiwane w trakcie realizacji przez gminę projektów współfinansowanych ze środków publicznych wymienionych w Art. 5 ust. 1 pkt 2 i 3 ustawy z dnia 27 sierpnia 2009r. O finansach publicznych (Dz. U. Nr 157 poz. 1240 z późn. zm.)
b) Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
c) Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
d) Kadra Kierownicza Urzędu Miejskiego w Sokółce jest odpowiedzialna za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur w całym systemie.

3 Zabezpieczenie dostępu do danych osobowych

Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych stanowi Załącznik nr 1 do niniejszej instrukcji.
W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych) jednak wymaga to zgody indywidualnej administratora bezpieczeństwa informacji. Szczegółowe zasady przetwarzania danych osobowych na komputerach przenośnych opisano w punkcie 8 niniejszej instrukcji.
Dostęp osób trzecich do pomieszczeń, w których przetwarzane są dane osobowe dozwolony jest wyłącznie w obecności pracownika posiadającego upoważnienie do przetwarzania danych osobowych.
Dostęp do pomieszczeń, w których znajdują się serwery baz danych lub przechowywane są kopie zapasowe dozwolony jest wyłącznie w obecności administratora bezpieczeństwa

informacji.
Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.

4 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Aktualny wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych znajduje się w Załączniku nr 2 do niniejszego dokumentu.
Załącznik ten powinien być aktualizowany po wprowadzeniu do przetwarzania nowych zbiorów danych osobowych lub nowych programów, które je obsługują.

5 Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Opis struktury zbiorów danych dostępny jest w dokumentacji poszczególnych systemów informatycznych, znajdującej się na stanowisku Administratora Bezpieczeństwa Informacji

6 Sposób przepływu danych pomiędzy poszczególnymi systemami

Aktualny opis sposobu przepływu danych pomiędzy poszczególnymi systemami znajduje się w dokumentacji dostępnej na stanowisku Administratora Bezpieczeństwa Informacji

7 Określenie środków technicznych i organizacyjnych

7.1 Zasady ogólne:

a) Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.
b) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
c) Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
d) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

7.2 Środki techniczne

a) Budynek urzędu jest zamykany po zakończeniu pracy i nadzorowany przez pracownika dozoru.
b) Główne ciągi komunikacyjne i otoczenie budynku są objęte całodobowym monitoringiem wizyjnym, obraz z kamer jest nagrywany na dyskach HDD i przechowywany przez 14 dni.
c) Pomieszczenia budynku są wyposażone w system alarmowy włączany bezpośrednio po zakończeniu pracy.
d) Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Bezpieczeństwa Informacji.

e) Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
f) W przypadku przebywania interesantów bądź innych osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

7.3 Środki organizacyjne

a) Wprowadzenie instrukcji dla pracowników zatrudnionych przy przetwarzaniu danych osobowych.
b) Powołanie Administratora Bezpieczeństwa Informacji, i Administratorów Systemu Informatycznego, odpowiedzialnych za działania organizacyjne i środki techniczne zapewniające odpowiedni poziom bezpieczeństwa danych osobowych. Funkcje Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego może pełnić jedna osoba.
c) Prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.
d) Kontrola dostępu do pomieszczeń, w których znajdują się serwery.
e) Zgodne z „Instrukcją zarządzania systemem" tworzenie kopii archiwalnych baz danych zawierających dane osobowe.
f) Testowanie modyfikacji oprogramowania przed wdrożeniem go do użytku operacyjnego zarówno pod kątem poprawności działania jak i podatności na „ataki" z zewnątrz..

7.4 Sposób postępowania w zakresie komunikacji w sieci komputerowej

Dane osobowe są przesyłane w sieci informatycznej dedykowanej do obsługi systemu informatycznego przetwarzającego te dane (intranet). Sieć ta jest odseparowana od pozostałej infrastruktury teleinformatycznej poprzez fizyczne rozdzielenie infrastruktury ethernetowej.
Ruch dla usług publicznych jest chroniony przy pomocy access-list na routerze, udostępniając tylko wybrane porty na serwerach znajdujących się w sieci. Ponadto, cały ruch do sieci dedykowanej przechodzi przez serwer pełniący rolę zapory ogniowej (firewall sprzętowy), gdzie jest filtrowany i translowany na lokalną klasę adresów. Dodatkowo serwery sieci lokalnej chronione przez własne zapory ogniowe (firewall) uniemożliwiające nieautoryzowany dostęp do danych znajdujących się na tych serwerach. Ponadto na każdej stacji roboczej zainstalowane jest zintegrowane oprogramowanie typu antywirus/firewall programowy/antyspam, w którym aktualizacja modułów i baz wirusów odbywa się nie rzadziej niż raz dziennie.

7.5 Zasady postępowania w przypadku naruszenia ochrony danych osobowych

Każdy pracownik biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogące spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania administratora bezpieczeństwa informacji lub administratora systemu informatycznego.
O naruszeniu ochrony danych osobowych mogą świadczyć następujące symptomy:
a) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp

b) do danych osobowych,
c) brak możliwości zalogowania się do tej aplikacji,
d) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
e) wygląd aplikacji inny niż normalnie,
f) inny zakres danych niż normalnie dostępny dla użytkownika – dużo więcej lub dużo mniej danych,
g) znaczne spowolnienie działania systemu informatycznego,
h) pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
i) ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
j) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych,
k) włamanie lub próby włamania do szafek, w których przechowywane są – w postaci elektronicznej lub papierowej – nośniki danych osobowych,
l) zagubienie bądź kradzież nośnika danych osobowych,
m) zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, dyskietki itp.),
n) kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
o) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
p) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,
q) podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

W wypadku wystąpienia powyższych symptomów, jak również innych objawów, które zdaniem pracownika mogą wskazywać na zagrożenie bezpieczeństwa danych osobowych, należy natychmiast powiadomić administratora bezpieczeństwa informacji lub administratora systemu informatycznego. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż administrator bezpieczeństwa informacji, jest ona zobowiązana poinformować o tym fakcie administratora bezpieczeństwa informacji.

Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w Urzędzie Miejskim w Sokółce naruszenia bezpieczeństwa danych osobowych administrator bezpieczeństwa informacji, we współpracy z administratorem systemu informatycznego, jest zobowiązany do podjęcia kroków w celu:

a) wyjaśnienia zdarzenia, a w szczególności czy miało miejsce naruszenie ochrony danych osobowych,
b) wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów, a w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,
c) zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się

zagrożenia,
d) usunięcia skutków incydentu i przywróceniu pierwotnego stanu systemu informatycznego (to jest stanu sprzed incydentu).

Administrator bezpieczeństwa informacji we współpracy z administratorem systemu informatycznego podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia:

a) przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego,
b) przeprowadzenie analizy danych osobowych przetwarzanych w systemie informatycznym,
c) zabezpieczenie danych przetwarzanych w systemie informatycznym,w szczególności danych konfiguracyjnych tego systemu.

Administrator bezpieczeństwa informacji określa na podstawie zebranych informacji przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, jest on zobowiązany do pisemnego powiadomienia administratora danych osobowych , który może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu. Administrator bezpieczeństwa informacji prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

a) imię i nazwisko osoby zgłaszającej incydent,
b) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
c) datę zgłoszenia incydentu,
d) przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
e) wyniki przeprowadzonych działań,
f) podjęte akcje naprawcze i ich skuteczność.

Administrator bezpieczeństwa informacji odpowiedzialny jest za przeprowadzanie okresowych analiz zaistniałych incydentów w celu:

a) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
b) określenie wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,
c) określenie potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

8 Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe

Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie za zgodą administratora danych osobowych i za wiedzą administratora bezpieczeństwa informacji. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala przełożony pracownika za wiedzą administratora bezpieczeństwa informacji.

Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób

nieupoważnionych oraz przed zniszczeniem. Użytkownik komputera przenośnego zobowiązany jest do:

a) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
- nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp,
- transportowania komputera w bagażu podręcznym
- zaleca się przenoszenie komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych.

b) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,

c) nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,

d) zabezpieczania komputera przenośnego hasłem,

e) blokowanie dostępu do komputera przenośnego w przypadku gdy nie jest on wykorzystywany przez pracownika,

f) kopiowanie danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych,

g) umożliwienia, poprzez podłączenie komputera do sieci informatycznej aktualizacji wzorców wirusów w programie antywirusowym,

h) utrzymanie konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł,

i) wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,

j) zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

Administrator bezpieczeństwa informacji zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności aby:

a) dokonano konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, wykorzystywanie haseł odpowiedniej jakości

b) zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe,

c) zabezpieczono dane osobowe przetwarzane na komputerach przenośnych poprzez zastosowanie oprogramowania szyfrującego te dane. Dostęp do danych jest możliwy wyłącznie po podaniu tego hasła,

d) dokonano instalacji i konfiguracji oprogramowania antywirusowego na komputerze przenośnym,

e) przeprowadzono aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

W razie zgubienia lub kradzieży pracownik zobowiązany jest do natychmiastowego powiadomienia administratora bezpieczeństwa informacji lub osoby uprawnionej zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

BURMISTRZ

Stanisław Małachwiej

Załącznik nr 2
Do Zarządzenie wewnętrznego Nr 05/10
Burmistrza Sokółki
z dnia 15.03.2010 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Spis treści

1. Definicje

a) 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.
b) Administrator danych osobowych - zadania administratora danych osobowych wykonuje Burmistrz Sokółki.
c) Administrator bezpieczeństwa informacji - osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych we wskazanych systemach informatycznych.
d) Administrator systemu informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w Urzędzie Miejskim w Sokółce (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).
e) System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu

przetwarzania danych.

f) Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
g) Bezpieczeństwo systemu informatycznego - wdrożenie przez administratora danych osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
h) Przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
i) Osoba upoważniona - osoba posiadająca upoważnienie wydane przez administratora danych osobowych i dopuszczona jako użytkownik do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.
j) Użytkownik systemu - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
k) Osoba uprawniona - osoba posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności.
l) Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych.
m) Rozporządzenie - rozporządzenie 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.

2. Informacje ogólne

Niniejsza instrukcja dotyczy każdego zbioru danych osobowych przetwarzanego w Urzędzie Miejskim w Sokółce zarówno w formie elektronicznej jak i papierowej. Aktualny wykaz przetwarzanych zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych i ich lokalizacją znajduje się w Załączniku 1 do dokumentu Polityka Bezpieczeństwa. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych w Urzędzie Miejskim w Sokółce stanowi załącznik nr 2 do dokumentu Polityka Bezpieczeństwa.

3. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych. Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego użytkownika. Składa on wniosek do Administratora danych osobowych o wydanie upoważnienia do przetwarzania danych osobowych. Wniosek ten powinien zawierać:

a) imię i nazwisko pracownika, któremu upoważnienie zostanie nadane,
b) nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
c) zakres upoważnienia do przetwarzania danych osobowych,

d) datę, z jaką upoważnienie ma być nadane,
e) okres ważności upoważnienia.

Upoważnienie sporządza się w trzech egzemplarzach, każdy na prawach oryginału. , które otrzymują: osoba upoważniona, administrator bezpieczeństwa informacji i pracownik ds. kadr. Wzór upoważnienia wraz z oświadczeniem pracownika stanowi załącznik nr 1 do niniejszego dokumentu.

Identyfikator i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych lub osobę przez niego uprawnioną. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator odpowiedniego systemu informatycznego. Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek administratora danych osobowych, przełożonego użytkownika lub koordynatora zadania, na rzecz którego były wykonywane czynności związane z przetwarzaniem danych osobowych.

Wniosek o wyrejestrowanie użytkownika systemu należy złożyć do Administratora danych osobowych. Wyrejestrowanie użytkownika z systemu realizuje administrator odpowiedniego systemu informatycznego na pisemny lub przesłany drogą elektroniczną wniosek administratora bezpieczeństwa informacji.

Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Urzędzie Miejskim w Sokółce. Zgodnie z art. 39 ust. 1 ustawy taka ewidencja zawiera:

a) imię i nazwisko osoby upoważnionej,
b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
c) nazwa systemu informatycznego, którego dotyczy upoważnienie,
d) identyfikator nadany w systemie.

4. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

a) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
b) Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
c) Identyfikator składa się minimalnie z czterech znaków, znaki identyfikatora nie są rozdzielone spacjami, identyfikator nie zawiera polskich liter,
d) Identyfikator wpisuje się do ewidencji, prowadzonej przez administratora bezpieczeństwa informacji, wraz z imieniem i nazwiskiem użytkownika oraz nazwami systemów informatycznych, do których użytkownik uzyskał dostęp i wprowadzany jest przez administratorów systemów informatycznych do właściwych systemów,
e) identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób

wymagający bezpieczne zarządzanie hasłami użytkowników:

a) hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego przetwarzającego dane osobowe,
b) hasła są zmieniane przez użytkownika,
c) system informatyczny wyposażony jest w mechanizmy pozwalający na wymuszające zmiany hasła po upływie 30 dni od dnia ostatniej zmiany hasła,
d) system informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła, w szczególności hasło powinno składać się z co najmniej 8 znaków.
e) Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne, do których mają przydzielone hasło. Zasady zarządzania hasłami są analogiczne, jak w przypadku haseł użytkowników.
Nazwy i hasła użytkowników posiadających uprawnienia administratorów systemów informatycznych powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie uprawnione osoby. Nazwy użytkowników oraz hasła powinny być przechowywane w opieczętowanej i opatrzonej podpisem administratorów systemu kopercie. W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniała sytuację w „Dzienniku haseł" znajdującym się w szafie wraz z kopertą, w której znajdują się hasła.
Wpis powinien zawierać następujące informacje:

a) imię i nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,
b) imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
c) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

W przypadku, gdy system informatyczny posiada możliwość zmiany hasła użytkownika przez administratora systemu informatycznego, dopuszcza się nie prowadzenie „Dziennika haseł".
O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony administrator bezpieczeństwa informacji.

5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka bezpieczeństwa" punkt 7.5.
Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z administratorem bezpieczeństwa informacji.
Użytkownik informuje administratora bezpieczeństwa informacji o zablokowaniu dostępu

do zbioru danych.
W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 10 minut automatycznie włączany jest wygaszacz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu. Hasło powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne oraz być zmieniane nie rzadziej niż co 30 dni.
Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.
W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.
Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

6. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego lub osoba specjalnie do tego celu wyznaczona. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegranie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze.
W przypadku, gdy z przyczyn technicznych jest to niemożliwe użytkownicy systemu są zobowiązani do sporządzania kopii zapasowych baz danych na nośniku wymiennym i centralne ich przechowywanie w miejscu wskazanym przez administratora bezpieczeństwa informacji.

Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:

a) kopia zapasowa danych osobowych przetwarzanych przez aplikację (pełna kopia) wykonywana jest codziennie na dysku serwera danych, lub na dysku lokalnym komputera wybranego przez administratora systemu informatycznego,
b) raz w miesiącu, w ostatnim dniu roboczym miesiąca, na nośniku wymiennym tworzona jest kopia zawierająca kopie dzienne,
c) zbiorcze (miesięczne) kopie przechowywane są przez okres czterech miesięcy, po tym terminie stare kopie są niszczone poprzez nadpisywanie ich przez bardziej aktualne,

d) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu – pełna kopia wykonywana jest raz w tygodniu, i przechowywana przez miesiąc, po czym nadpisywana jest nową wersją kopii, przechowywana jest w zamkniętej szafie.

Do tworzenia kopii zapasowych wykorzystywane są dedykowane do tego celu urządzenia wchodzące w skład systemu informatycznego na nośnikach wymiennych adekwatnych do rodzaju urządzenia.
W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, których to dotyczy muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator systemu informatycznego. Z przeprowadzonego testu administrator systemu sporządza krótką notatkę uwzględniającą datę testu oraz jego rezultat (kopię notatki przekazuje administratorowi bezpieczeństwa informacji). Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

7. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w § 5 pkt 4 rozporządzenia

Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza budynek Urzędu Miejskiego powinno odbywać się za wiedzą administratora bezpieczeństwa informacji.
W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami umieszczonymi w punkcie 5. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów. W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona zgodnie ze wskazówkami umieszczonymi w punkcie 6.

8. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania,o którym mowa w pkt III załącznika do rozporządzenia.

W związku z tym, że system informatyczny narażony jest na działanie oprogramowania,, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu konieczne jest podjęcie odpowiednich środków ochronnych.
Można wyróżnić następujące rodzaje występujących tu zagrożeń:

a) nieuprawniony dostęp bezpośrednio do bazy danych,
b) uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
c) przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet,
d) przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
e) uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

a) fizyczne odseparowanie serwera bazy danych od sieci zewnętrznej,
b) autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
c) stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,
d) stosowanie aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
e) stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

a) załączniki do poczty elektronicznej,
b) przeglądane strony internetowe,
c) pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego przetwarzającego dane osobowe, lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

a) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
b) antywirusowy skaner ruchu internetowego powinien być stale włączony,
c) monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony,
d) skaner poczty elektronicznej powinien być stale włączony.

Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane

w sposób następujący:

a) zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
b) możliwość centralnego uaktualnienia wzorców wirusów.
c) Możliwość centralnego zarządzania systemem antywirusowym z poziomu konsoli zarządzania zainstalowanej na serwerze.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

Użytkownicy systemu informatycznego zobowiązani są do następujących działań:

a) skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przynajmniej razy w tygodniu,
b) skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej przy każdym użyciu
c) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
b) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
c) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej:

a) filtry zabezpieczające stacje robocze przed skutkami przepięcia,
b) zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamkniecie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

9. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia

System informatyczny przetwarzający dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

a) rozpoczęcie i zakończenie pracy przez użytkownika systemu,

b) operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie,modyfikację oraz usunięcie,
c) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
d) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
e) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

Zapis działań użytkownika uwzględnia:

a) identyfikator użytkownika,
b) datę i czas, w którym zdarzenie miało miejsce,
c) rodzaj zdarzenia,
d) określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

W ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na automatyczne powiadomienie administratora bezpieczeństwa informacji lub osoby przez niego uprawnionej o zaistnieniu zdarzenia krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych).

10. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
Prace serwisowe na terenie Urzędu Miejskiego prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników urzędu lub przez upoważnionych przedstawicieli wykonawców zewnętrznych znajdujących się w towarzystwie pracowników urzędu.
Przed rozpoczęciem prac serwisowych przez osoby spoza Urzędu Miejskiego konieczne jest potwierdzenie tożsamości serwisantów. Dopuszczalne też są zdalne prace serwisowe, pod warunkiem posiadania przez serwisanta imiennego upoważnienia do przetwarzania danych osobowych wydanego przez administratora danych.
Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

BURMISTRZ
Stanisław Małachwiej

Załącznik Nr 1
do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Sokółce

UPOWAŻNIENIE
do przetwarzania danych osobowych

I.

Upoważniam Panią/Pana .....
(imię i nazwisko)

zatrudnioną/zatrudnionego w .....

.....
(nazwa jednostki komórki organizacyjnej)

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku:

.....
(zajmowane stanowisko)

oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład.
Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.*) i elektronicznej, wg wykazu zbiorów podanych w pkt. II.

II.

Upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w następujących zbiorach:
1.....
2.....
3.....

OŚWIADCZENIE PRACOWNIKA

III.

Ja niżej podpisana (*ny*) oświadczam, iż:

1. Zostałam (*em*) przeszkolona (*ny*) w zakresie ochrony danych osobowych i znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych t.j. Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm. oraz **„Polityką Bezpieczeństwa"** i **„Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"**
2. Zobowiązuję się:

- zachować w tajemnicy dane osobowe, z którymi zetknęłam się / zetknąłem się* w trakcie wykonywania swoich obowiązków służbowych, zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu;
- chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych, zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem.

3. Znana jest mi odpowiedzialność karna za naruszenie ww. ustawy (art. 49-54).

.....
(podpis Administratora Danych)

.....
(data, podpis pracownika)

Uwaga:
- niniejsze upoważnienie zostało sporządzone w trzech jednobrzmiących egzemplarzach – każdy na prawach oryginału, które otrzymują:
1. Osoba upoważniona;
2. Kadry - do akt osobowych upoważnionego;
3. Administrator Bezpieczeństwa Informacji

*) *niepotrzebne skreślić.*