

ZARZĄDZENIE Nr 53.2014

Wójta Gminy Zawady
z dnia 5 czerwca 2014 roku.

w sprawie ochrony danych osobowych w Urzędzie Gminy Zawady.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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. Wprowadza się „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Zawady” stanowiącą załącznik nr 1 do zarządzenia.
2. Wprowadza się „Instrukcję zarządzania systemem informatycznym w Urzędzie Gminy Zawady” stanowiącą załącznik Nr 2 do zarządzenia.
- § 2. Traci moc Zarządzenie Nr 49/07 Wójta Gminy Zawady z dnia 20 listopada 2007 roku w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych systemu informatycznego Urzędu Gminy w Zawadach oraz dokumentów dotyczących ochrony danych osobowych w Urzędzie.
- § 3. Zarządzenie wchodzi w życie z dniem podpisania.

WYWIESZONO NA TABLICY OGŁOSZENI
UG. ZAWADY ORAZ OPUBLIKOWANO W
BIP-ie UG. ZAWADY DN. 10. 06. 2014 R.
Grzegorz Rych
ST. INSPEKTOR
UG. ZAWADY

Wójt Gminy Zawady

/-/ Krzysztof Wądołowski

Krzysztof Wądołowski

NK REJ. REF. O.O. 160. 2014 R.
(10. 06. 2014 R.)

Załącznik Nr 1 do Zarządzenia Nr 53.2014

Wójta Gminy Zawady

z dnia 5 czerwca 2014 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH w Urzędzie Gminy Zawady

Rozdział 1.

Postanowienia ogólne

1. Podstawa prawna

Podstawę prawną dla polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Zawady stanowią: Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (tekst jednolity: Dz. U.2002 r. Nr 101 poz. 926, ze zm.), 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 (Dz. U. Nr. 100, poz. 1024).

2. Wstęp.

Celem Polityki bezpieczeństwa przetwarzania danych osobowych jest zabezpieczenie przetwarzania informacji stanowiących dane osobowe w rozumieniu ustawy o ochronie danych osobowych.

3. Obszar przetwarzania danych osobowych.

- 1) obszar przetwarzania danych osobowych stanowi siedziba Urzędu Gminy Zawady Plac Wolności 12 oraz pomieszczenie, w którym przetwarzane są dane osobowe z użyciem sprzętu komputerowego lub w formie kartotek, ksiąg, skorowidzów i innych.
- 2) pomieszczenie, w którym przetwarzane są dane osobowe, na czas nieobecności w nich osób upoważnionych do przetwarzania danych muszą być zamykane w sposób uniemożliwiający dostęp do nich osobom postronnym,
- 3) wewnątrz obszaru, o którym mowa w § 1 osoby postronne mogą przebywać wyłącznie w obecności osób upoważnionych do przetwarzania danych osobowych,
- 4) w pomieszczeniach, w których przebywają osoby postronne monitory stanowisk dostępu powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

4. Wykaz zbiorów danych osobowych .

Referat Finansowy

1. Podatki i opłaty lokalne.

Referat Organizacyjny

1. Oświadczenia majątkowe.

Referat Rolnictwa, Ochrony Środowiska i Obsługi Technicznej.

1. Zamówienia Publiczne.

Urząd Stanu Cywilnego

1. Akta Stanu Cywilnego.
2. Ewidencja ludności i dowody osobiste.
3. Rejestracja przedpoborowych.

Ośrodek Pomocy Społecznej.

1. Pomoc społeczna.
2. Dodatki mieszkaniowe.

5.. Definicje stosowanych pojęć

- 1) dane osobowe– wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby,
- 2) osoba możliwa do zidentyfikowania – każda osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,
- 3) zbiór danych– każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
- 4) komputerowy zbiór danych– zbiór danych osobowych w formie elektronicznej,
- 5) tradycyjny zbiór danych – zbiór danych osobowych w formie papierowej (np. książki, wykazy, ewidencje),
- 6) przetwarzanie danych– jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
- 7) Urząd– Urząd Gminy Zawady z siedzibą: 16-075 Zawady, Plac Wolności 12,
- 8) Administrator Danych Osobowych– Wójt Gminy Zawady reprezentujący Urząd, który decyduje o celach i środkach przetwarzania danych osobowych oraz monitoruje wdrożone zabezpieczenia systemu informatycznego,
- 9) Administrator Bezpieczeństwa Informacji– osoba nadzorująca przestrzeganie zasad przetwarzania i ochrony danych osobowych,
- 10) Informatyk– osoba odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych w Urzędzie, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach,
- 11) osoba upoważniona– osoba posiadająca upoważnienie do przetwarzania danych osobowych w określonym zakresie wydane przez Administratora Danych Osobowych,
- 12) osoba uprawniona– osoba upoważniona lub inna osoba uprawniona do przetwarzania danych osobowych

na podstawie szczególnych przepisów prawa ,

13) osoba trzecia – każda osoba nieuprawniona do przetwarzania danych osobowych będących w posiadaniu Administratora Danych Osobowych, a także osoba posiadająca upoważnienie

wydane przez Administratora Danych Osobowych, ale podejmująca czynności w zakresie przekraczającym zakres jej upoważnienia,

14) użytkownik– osoba upoważniona do przetwarzania danych osobowych w określonym zakresie w systemie informatycznym,

15) stacja robocza- stacjonarny lub przenośny komputer, umożliwiający użytkownikowi dostęp do danych przetwarzanych w formie elektronicznej,

16) zewnętrzne nośniki danych- przedmiot fizyczny służący do zapisywania, przechowywania, przetwarzania i transmisji danych (np. pendrive, CD, DVD),

17) system informatyczny– zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

18) zakres czynności– zakres czynności, upoważnień, odpowiedzialności i zastępstwa wynikającego ze stanowiska służbowego i pełnionego stanowiska,

19) zabezpieczenie systemu informatycznego – wdrożone przez Administratora Bezpieczeństwa Informacji oraz Informatyka odpowiednie środki organizacyjne i techniczne w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez użytkownika lub osobę trzecią.

Rozdział 2.

Cel i zakres polityki bezpieczeństwa danych osobowych

1. Cel polityki bezpieczeństwa

2. Celem niniejszej Polityki jest określenie kierunków działań oraz wsparcia dla zapewnienia bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Zawady.

3. Przez bezpieczeństwo danych osobowych rozumie się zapewnienie ich poufności, integralności i dostępności oraz zapewnienie przejrzystości działań podejmowanych zgodnie z niniejszą Polityką.

4. Urząd zarządza bezpieczeństwem danych osobowych w celu:

1) zapewnienia sprawnego i zgodnego z przepisami prawa wykonywania swoich zadań oraz zadań realizowanych na podstawie umów lub porozumień,

2) minimalizacji ryzyk w obszarze przetwarzania i ochrony danych osobowych wymienionych w Załączniku nr 1.

2. Zakres polityki bezpieczeństwa

1. Zakres przedmiotowy niniejszej Polityki obejmuje dane osobowe przetwarzane w Urzędzie, zarówno w formie elektronicznej, jak i tradycyjnej.

2. Procedury i zasady określone w niniejszej Polityce stosuje się do wszystkich pracowników Urzędu, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Urzędzie (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, wolontariuszy, stażystów, praktykantów, serwisantów).

1. Administrator Danych Osobowych zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym, pozyskaniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator Danych Osobowych przetwarza dane osobowe zgodnie z prawem oraz realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
 - 1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem zmian w obowiązującym prawie, organizacji Urzędu oraz technik zabezpieczenia danych osobowych, w szczególności o:
 - a) zbieraniu danych osobowych wyłącznie dla oznaczonych, przewidzianych prawem celów,
 - b) przetwarzaniu danych osobowych w postaci umożliwiającej identyfikację osób, których dotyczą,
 - c) informowaniu osoby, której dane zostały umieszczone w zbiorze danych, o przysługujących jej prawach, zgodnie z pkt 11 niniejszej Polityki,
 - d) przetwarzaniu danych osobowych nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
 - e) zapewnieniu kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane,
 - f) udostępnianiu danych osobowych innym podmiotom wyłącznie w sposób zgodny z prawem.
 - 2) nadaje upoważnienia do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi czynności, oraz prowadzi ich ewidencję,
 - 3) zgłasza zbiory danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem zbiorów ustawowo zwolnionych,
 - 4) wyznacza Administratora Bezpieczeństwa Informacji oraz określa jego zakres czynności,
 - 5) zleca Sekretarzowi Gminy, by we współpracy z Administratorem Bezpieczeństwa Informacji zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych,
 - 6) w razie stwierdzenia lub podejrzenia naruszenia zasad przetwarzania i ochrony danych osobowych, a w szczególności zabezpieczeń systemu informatycznego, na wniosek Administratora Bezpieczeństwa Informacji podejmuje odpowiednie działania w celu usunięcia zagrożenia lub minimalizacji jego skutków,
 - 7) udostępnia dane osobowe ze zbioru na żądanie uprawnionych podmiotów w przypadkach wskazanych prawem.

2. Administrator Bezpieczeństwa Informacji

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad przetwarzania i ochrony danych osobowych w imieniu i na rzecz Administratora Danych Osobowych.
2. W szczególności Administrator Bezpieczeństwa Informacji jest odpowiedzialny za: prowadzenie oraz aktualizację dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, tj.:
 - a) „Polityki bezpieczeństwa danych osobowych”, zawierającej między innymi:

- wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania,
- b) „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”
- 1) nadzorowanie przestrzegania zasad określonych w „Polityce bezpieczeństwa danych osobowych” i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”,
- 2) szkolenie osób dopuszczonych do przetwarzania danych osobowych lub przebywania w obszarze przetwarzania danych osobowych z zakresu zasad przetwarzania i ochrony tych danych oraz zasad bezpieczeństwa informatycznego w oparciu o przygotowywane przez siebie materiały szkoleniowe oraz prowadzenie adekwatnej dokumentacji w tym zakresie (np. potwierdzenie przeszkolenia),
- 3) nadzorowanie prawidłowości udostępniania danych osobowych odbiorcom danych,
- 4) nadzorowanie zamieszczania w umowach z użytkownikami upoważnionymi do przetwarzania danych osobowych, firmami, którym powierzono przetwarzanie danych osobowych lub konserwację urządzeń służących do przetwarzania danych oraz pracownikami tych firm, a także w innych dokumentach odpowiednich zapisów dotyczących ochrony danych osobowych,
- 5) nadzorowanie wdrożenia adekwatnych do zagrożeń środków fizycznych, a także organizacyjnych i technicznych służących zapewnieniu bezpieczeństwa,
- 6) nadzorowanie obiegu oraz przechowywania dokumentów zawierających dane osobowe w zakresie związanych z bezpieczeństwem tych danych osobowych,
- 7) koordynowanie kontroli wewnętrznych z zakresu przestrzegania przepisów o ochronie danych osobowych, w tym prowadzenie szczegółowej dokumentacji z kontroli dot.:
 - a) zakresu przestrzegania przepisów o ochronie danych osobowych,
 - b) stwierdzonych naruszeń bezpieczeństwa danych osobowych, obejmującej między innymi. analizę sytuacji, okoliczności przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło).
- 3. podejmowanie lub wnioskowanie o podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego oraz prowadzenie adekwatnej dokumentacji w tym zakresie (np. opis incydentu, dokumentacja dot. reakcji na incydent).

3. Informatyk

Informatyk realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych Osobowych, w szczególności:

- 1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora,
- 2) Zarządza systemem komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji,
- 3) nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych oraz kontroli dostępu do danych osobowych,
- 4) wykonuje kopie bezpieczeństwa komputerowych zbiorów danych zgodnie z zasadami określonymi w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”, oraz okresowo sprawdza je pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii

systemu informatycznego,

5) przydziela każdemu użytkownikowi indywidualny identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także w porozumieniu z sekretarzem miasta usuwa konta użytkowników zgodnie z zasadami określonymi w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”,

6) zmienia okresowo hasła dostępu użytkowników do systemu informatycznego w przypadkach, gdy system informatyczny nie wymusza okresowej zmiany haseł użytkowników określone w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”,

7) osobiście wykonuje lub sprawuje nadzór nad wykonywaniem: napraw, konserwacji oraz likwidacji urządzeń komputerowych, które mogą zawierać dane osobowe.

4. Sekretarz gminy realizuje następujące zadania w zakresie ochrony danych osobowych:

1) występuje z wnioskiem do Administratora Danych Osobowych o nadanie, modyfikację lub odwołanie upoważnienia do przetwarzania danych osobowych,

2) prowadzi ewidencję upoważnień do przetwarzania danych osobowych,

3) przechowuje upoważnienia do przetwarzania danych osobowych w aktach osobowych,

4) informuje Administratora Bezpieczeństwa Informacji o nadaniu, modyfikacji lub odwołaniu przez Administratora Danych Osobowych upoważnienia do przetwarzania danych osobowych,

5) nadzoruje wykonywanie kopii bezpieczeństwa komputerowych zbiorów danych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,

6) nadzoruje przeprowadzanie przeglądów, konserwacji oraz uaktualniania systemów służących do przetwarzania danych osobowych oraz wszystkich innych czynności wykonywanych przez Informatyków na komputerowych zbiorach danych.

5. Kierownicy referatów są odpowiedzialni za:

1) nadzorowanie przestrzegania zasad przetwarzania i ochrony danych osobowych przyjętych w Urzędzie przez podległy personel, w szczególności:

a) przetwarzania danych osobowych w celu i zakresie określonym w imiennym upoważnieniu do przetwarzania danych osobowych,

b) stosowania przydzielonych im indywidualnych identyfikatorów dostępu do systemu informatycznego przez podległych pracowników,

c) przeciwdziałania dostępowi osób nieuprawnionych do danych osobowych i systemu informatycznego, w którym są przetwarzane,

d) prawidłowego zabezpieczania danych osobowych oraz miejsc ich przechowywania w trakcie i po zakończeniu pracy,

2) niedopuszczenie do używania zewnętrznych nośników danych do celów innych niż niezbędne do realizacji zadań referatu lub tworzenia kopii bezpieczeństwa, z wyjątkiem sytuacji gdy jest to niezbędne ze względu na specyfikę zadania,

3) współdziałanie z Administratorem Bezpieczeństwa Informacji w zakresie przestrzegania zasad

przetwarzania i ochrony danych osobowych w Urzędzie Gminy oraz identyfikacji i analizy ryzyk związanych z tym przetwarzaniem,

4) niezwłoczne informowanie Administratora Bezpieczeństwa Informacji, o każdym stwierdzeniu lub podejrzeniu naruszenia bezpieczeństwa danych osobowych lub systemu informatycznego, w którym są przetwarzane oraz współdziałanie przy usuwaniu skutków takiego naruszenia.

6. Osoby przetwarzające dane osobowe

1. Każda osoba przetwarzająca dane osobowe posiada odpowiednie upoważnienie do przetwarzania danych osobowych zawierające: imię i nazwisko, datę nadania i okres jego obowiązywania, zakres danych, które osoba może przetwarzać (zbiory danych) oraz identyfikator w przypadku gdy dane osobowe są przetwarzane w systemie informatycznym.

2. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do:

1) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków,

2) poznania i bezwzględnego przestrzegania obowiązujących u Administratora Danych Osobowych zasad przetwarzania i ochrony danych osobowych oraz bezpieczeństwa systemu informatycznego,

3) zachowania w tajemnicy danych, które przetwarza oraz sposobów ich zabezpieczenia przez cały okres zatrudnienia u Administratora Danych Osobowych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,

4) korzystania z systemu informatycznego Administratora Danych Osobowych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników oraz zasadami przyjętymi w Urzędzie,

5) zabezpieczania danych osobowych oraz informacji o zabezpieczeniach systemu informatycznego przed ich udostępnianiem osobom nieuprawnionym, nieuprawnioną modyfikacją, utratą lub zniszczeniem.

7. Osoby, których dane dotyczą

1. Każdej osobie, której dotyczą dane osobowe przetwarzane u Administratora Danych Osobowych, przysługuje prawo do:

1) dostępu do treści przetwarzanych danych osobowych tej osoby,

2) poprawiania treści przetwarzanych danych osobowych tej osoby (bez zbędnej zwłoki), tj. do uzupełnienia, uaktualnienia, sprostowania danych osobowych, a także żądania czasowego lub trwałego wstrzymania ich przetwarzania bądź usunięcia ze zbioru, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy, albo są już zbędne dla realizacji celu, dla którego zostały zebrane,

3) kontroli przetwarzanych danych osobowych tej osoby, w szczególności uzyskania informacji o:

a) istnieniu zbioru danych osobowych i jego administratorze (wraz z siedzibą),

b) celu, zakresie i sposobie przetwarzania danych osobowych,

c) terminie rozpoczęcia przetwarzania danych osobowych w zbiorze,

d) treści jej danych osobowych (podanej w powszechnie zrozumiałej formie),

d) źródle, z jakiego pochodzą te dane (chyba że Administrator Danych Osobowych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej),

którym dane są udostępniane),

f) przesłankach podjęcia rozstrzygnięcia indywidualnej sprawy uwzględniającej wniosek osoby, której dane dotyczą, podjętego podczas zawierania lub wykonywania umowy wyłącznie na podstawie operacji na danych osobowych prowadzonych w systemie informatycznym,

g) obowiązku lub dobrowolności podania danych, a także jeśli taki obowiązek istnieje – o jego podstawie prawnej,

h) prawie dostępu do treści swoich danych i ich poprawiania, o których mowa w pkt. 1 i 2,

i) wniesienia sprzeciwu wobec ich wykorzystania w celach marketingowych lub przekazania innemu administratorowi danych (z uwzględnieniem wyjątków ustawowych),

j) udzielenia informacji o przysługujących prawach osobie, której dane dotyczą, na jej wniosek w terminie 30 dni.

2. W przypadku zbierania danych osobowych bezpośrednio od osoby, której one dotyczą, na jej żądanie udziela się informacji wskazanych w ust. 1 pkt 3 lit. a-f, ale nie częściej niż raz na 6 miesięcy.

3. Informacja, o której mowa w ust. 1 pkt. 3, powinna być udzielana w zrozumiałej formie oraz na piśmie, jeśli osoba o to wnioskuje.

4. W przypadku, gdy w niedużym odstępie czasowym dochodzi do ponownego lub kolejnego zbierania danych tej samej osoby do tych samych celów, można powołać się na fakt wcześniejszego udzielenia informacji, o których mowa w ust. 1 pkt. 3.

5. Obowiązek informacyjny nie występuje w przypadku, gdy:

1) ze względu na okoliczności przekazania danych osobowych do przetwarzania w zbiorze zachodzi pewność (tj. obiektywna świadomość), że osoba, której dane dotyczą, posiada wszystkie informacje, o których mowa w ust. 1 pkt 3,

2) dane są przetwarzane dla celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, a udzielenie informacji pociągałoby za sobą nakłady niewspółmierne z zamierzonym celem,

3) przekazanie informacji spowodowałoby:

a) ujawnienie wiadomości zawierających informacje niejawne,

b) zagrożenie dla obronności lub bezpieczeństwa państwa, życia lub zdrowia ludzi lub bezpieczeństwa publicznego,

c) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa, istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

Rozdział 4

Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i przejrzystości przetwarzanych danych osobowych

1. Zachowanie poufności

1. W przypadku naboru na wolne stanowiska należy zwracać uwagę między innymi na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.

2. Ryzyko utraty bezpieczeństwa danych przetwarzanych przez Administratora Danych Osobowych, pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci, usługodawcy), jest minimalizowane przez wprowadzanie do podpisanych umów zapisów o powierzeniu przetwarzania danych osobowych.

3. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. konserwatorzy i osoby sprząające pomieszczenia Administratora Danych Osobowych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

2. Środki techniczne i organizacyjne niezbędne do zapewnienia bezpieczeństwa przetwarzanych danych.

A. Środki ochrony fizycznej .

1. Budynek, w którym zlokalizowany jest obszar przetwarzania danych osobowych po godzinach urzędowania zabezpieczony za pomocą całodobowego monitoringu.

Urządzenia służące przetwarzaniu danych osobowych znajdują się w zamkniętych pomieszczeniach.

Wejście do budynku zamykane jest na dwa zamki.

Drzwi do pokoi zamykane są na zamki.

B. Środki organizacyjne.

1. Sekretariat Urzędu prowadzi ewidencję osób dopuszczonych do przetwarzania danych osobowych.

Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do przetwarzania tych danych podpisują:

- a) upoważnienie do przetwarzania danych załącznik nr 1,
- b) oświadczenie o znajomości przepisów dotyczących przetwarzania danych osobowych,
- c) oświadczenie o zachowaniu danych w tajemnicy załącznik nr 2.

3. Szkolenia w zakresie ochrony danych osobowych

1. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za szkolenie:

- 1) każdej osoby, która ma zostać dopuszczona do przetwarzania danych osobowych,
- 2) wszystkich osób upoważnionych do przetwarzania danych osobowych w przypadku:
 - a) zmiany zasad przetwarzania i ochrony danych osobowych,
 - b) stwierdzenia istotnych lub powtarzalnych naruszeń zasad przetwarzania i ochrony danych osobowych lub naruszenia bezpieczeństwa systemu informatycznego,
- 3) osób dopuszczonych do przebywania w obszarze przetwarzania danych osobowych,
- 4) osób innych niż upoważnione do przetwarzania danych osobowych, jeśli pełnione przez nie funkcje wiążą się z przetwarzaniem i ochroną danych osobowych.

2. Tematyka szkoleń jest dostosowana do stanowiska/funkcji danej osoby i obejmuje:

- 1) zasady przetwarzania i ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i/lub zapisów na zewnętrznych nośnikach danych,

- 2) sposoby ochrony danych osobowych przed osobami nieuprawnionymi i procedury udostępniania danych osobom, których one dotyczą,
- 3) obowiązki osób upoważnionych do przetwarzania danych osobowych,
- 4) odpowiedzialność za naruszenie zasad przetwarzania i ochrony danych osobowych,
- 5) zasady powiadamiania i reakcji na stwierdzenie lub podejrzenie naruszenia zasad przetwarzania i ochrony danych osobowych,
- 6) zasady i procedury określone w „Polityce bezpieczeństwa danych osobowych” i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

4. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

1. Niezastosowanie się do obowiązujących u Administratora Danych zasad bezpieczeństwa danych osobowych, w szczególności świadome naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych, może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

2. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego. Możliwość popełnienia przestępstwa może zaistnieć w skutek :

- 1) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,
- 2) niezabezpieczenia nośnika lub komputera przenośnego,
- 3) zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym Administratora Danych Osobowych.

3. W przypadku stwierdzenia naruszenia zabezpieczeń systemu informatycznego należy postępować z zgodnie z „Instrukcją postępowania w przypadku naruszenia zabezpieczenia systemu informatycznego”.

5. Przeglądy i aktualizacje „Polityki bezpieczeństwa danych osobowych”

1. Niniejsza Polityka podlega przeglądowi pod kątem aktualności i stosowności nie rzadziej niż raz do roku. Przeglądu dokonuje Administrator Bezpieczeństwa Informacji.

2. Niniejsza Polityka podlega aktualizacji każdorazowo w przypadku:

- 1) likwidacji, utworzenia lub zmiany zawartości informacyjnej zbioru,
- 2) zmiany lokalizacji zbioru,
- 3) zmiany opiekuna zbioru lub administratora informacji,
- 4) zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji niniejszej Polityki,
- 5) innych znaczących zmian w funkcjonowaniu Urzędu dotyczących danych osobowych.

3. Aktualizacji niniejszej Polityki dokonuje Administrator Bezpieczeństwa Informacji. Zatwierdzenia zaktualizowanej Polityki dokonuje Administrator Danych Osobowych.

4. Administrator Bezpieczeństwa Informacji po uzgodnieniu z Administratorem Danych Osobowych może, stosownie do potrzeb, przeprowadzić wewnętrzną kontrolę zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Zakres, przebieg i rezultaty kontroli są dokumentowane na piśmie w protokole podpisywanym przez Administratora Bezpieczeństwa Informacji i Administratora Danych Osobowych.

Rozdział 5

Postanowienia końcowe

1. Niniejsza Polityka zostaje wprowadzona zarządzeniem Wójta Gminy Zawady.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszym dokumentem przed dopuszczeniem do przetwarzania danych oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

WÓJT
Krzysztof Wądołowski

OŚWIADCZENIE

Ja niżej podpisany.....syn
ur..... oświadczam, że zobowiązuje się do zachowania tajemnicy informacji
dotyczących danych osobowych uzyskanych w czasie pracy na stanowisku

Podstawa prawna: Dz. U. Nr 133 art. 39.

.....

Wójt Gminy

.....

podpis składającego oświadczenie

Załącznik Nr 2

do „Polityki Bezpieczeństwa”

UPOWAŻNIENIE

Upoważniam..... zatrudnionego na stanowisku
w referacie Urzędu Gminy do obsługi systemu informatycznego
służącego do przetwarzania danych osobowych.

.....

podpis osoby upoważniającej

Pouczenie:

Osoba upoważniona obowiązana jest do zachowania w tajemnicy informacji uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych.

Podstawa prawna: Dz. U. Nr 133. art. 37 i art. 39.

Przyjęłam /em do wiadomości i stosowania.

.....

data i podpis pracownika

**INSTRUKCJA
POSTĘPOWANIA W PRZYPADKU STWIERDZENIA NARUSZENIA ZABEZPIECZENIA
SYSTEMU INFORMATYCZNEGO**

1. Postanowienia ogólne .

1. Instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzonych i przetwarzania zarówno w zbiorach informatycznych, jak i w zbiorach przetwarzanych tradycyjnie. Instrukcję stosuje się także w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego i zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.

2. Przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy o ochronie danych i rozporządzeń wykonawczych, przetwarzanie danych (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie) oraz usuwanie (zmiana lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą).

3. Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie są:

- pracownicy upoważnieni do przetwarzania danych osobowych,
- kierownicy komórek organizacyjnych,
- administrator bezpieczeństwa informacji – w przypadku naruszenia systemów informatycznych.

II. Tryb postępowania w sytuacji naruszenia ochrony danych osobowych.

1. Każdy pracownik, który podejmie wiadomość lub stwierdzi naruszenie ochrony danych osobowych, jest zobowiązany do natychmiastowego poinformowania o tym bezpośredniego przełożonego, a gdy dotyczy to danych utrwalonych w zbiorach informatycznych administratora bezpieczeństwa informacji.

2. Gdy stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci teleinformatycznej mogą wskazać na naruszenie zabezpieczenia tych baz, to fakt ten należy zgłosić administratorowi bezpieczeństwa informacji.

3. Administrator bezpieczeństwa informacji razem z kierownikiem komórki organizacyjnej doraźnie usuwają przyczynę naruszenia systemu informatycznego, sprawdzają cały system.

4. W przypadku naruszenia bezpieczeństwa danych osobowych w zbiorach naturalnych kierownik komórki organizacyjnej sporządza protokół, który powinien zawierać:

- kto zgłosił, kiedy(data), o której godzinie,
- na czym polega naruszenie ochrony danych osobowych,
- zabezpieczone dowody naruszenia danych,
- propozycje wniosków co do dalszego trybu postępowania, w tym dotyczących zmiany systemu ochrony danych.

5. Protokół przedstawia się niezwłocznie Wójtowi Gminy.

6. Kierownik jednostki wdraża postępowanie wyjaśniające. Jeżeli stwierdzone zostanie naruszenie ochrony danych osobowych z winy pracownika wszczyna się postępowanie dyscyplinarne (wg odrębnych przepisów). Jeżeli naruszenie ochrony danych wyczerpuje znamiona przestępstwa określone w art. 49-52 i 54 ustawy sporządza się doniesienie (wniosek) do odpowiednich organów ścigania.

7. Administrator bezpieczeństwa informacji przeprowadza niezwłocznie analizę systemu i wprowadza dodatkowe zabezpieczenia w celu zmniejszenia zagrożenia i podatności systemu komputerowego na naruszenie bezpieczeństwa informacji.

INSTRUKCJA

OKREŚLAJĄCA SPOSÓB ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W URZĘDZIE GMINY ZAWADY

1. Cel instrukcji

Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją”, stanowi wykonanie obowiązku, o którym mowa w § 9 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).

2. Zakres instrukcji

Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, a w szczególności: sposób rejestrowania i wyrejestrowania użytkownika, sposób przydziału haseł i zasady korzystania z nich, procedury rozpoczęcia i zakończenia pracy, obowiązki użytkownika, metodę i częstotliwość tworzenia kopii, zasady sprawdzania obecności wirusów komputerowych oraz dokonywania przeglądów i konserwacji systemu.

3. Określenie obszaru przetwarzania danych

1. Obszar przetwarzania danych stanowią pokoje Urzędu Gminy Zawady, w których przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego i laptopów.

2. Wszystkie pomieszczenia, które należą do obszaru przetwarzania danych są zamykane na klucz. W czasie, gdy nie znajdują się w nich osoby upoważnione, pomieszczenia są zamykane w sposób uniemożliwiający wstęp osobom nieupoważnionym. Osoby nieupoważnione mogą przebywać w obszarze przetwarzania danych tylko za zgodą administratora danych lub w obecności osób upoważnionych.

3. Klucze do pomieszczeń, w których przetwarzane są dane osobowe są przechowywane w wyznaczonym miejscu w pomieszczeniu sekretariatu w szafce zamykanej na klucz.

4. Procedura wydawania upoważnień do przetwarzania danych osobowych

1. Użytkownikiem systemu informatycznego przetwarzającego dane osobowe (osobą upoważnioną) może być:

- a) osoba zatrudniona w Urzędzie Gminy Zawady i jednostkach podległych, która posiada upoważnienie Wójta Gminy,
- b) pracownik innego podmiotu lub przedsiębiorca będący osobą fizyczną prowadzącą działalność na podstawie wpisu do ewidencji działalności gospodarczej, którzy świadczą na podstawie stosowanych umów usługi związane z ich pracą w systemie informatycznym (serwis, zlecenie przetwarzania danych osobowych itp.) oraz posiadają upoważnienie Wójta Gminy do przetwarzania danych osobowych.

2. Upoważnienia do przetwarzania danych osobowych wydaje Wójt Gminy.
3. Wójt Gminy prowadzi ewidencję osób upoważnionych do ich przetwarzania.
4. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia.
5. Uprawnienia do programów aplikacyjnych rejestruje administrator danych zgodnie z udzielonym upoważnieniem do przetwarzania danych osobowych.
6. W przypadku zakończenia pracy w Urzędzie Gminy wygasa upoważnienie do przetwarzania danych osobowych. Administrator bezpieczeństwa informacji niezwłocznie usuwa uprawnienia do przetwarzania danych w systemie informatycznym.

5. Mechanizmy uwierzytelnienia użytkownika systemu

1. Każdorazowe uwierzytelnienie użytkownika w systemie następuje po podaniu hasła.
2. Używanie hasła jest obowiązkowe dla każdego użytkownika, posiadającego identyfikator w systemie.
3. W Urzędzie Gminy Zawady obowiązują następujące zasady korzystania z haseł:
 - hasła składają się co najmniej z ośmiu znaków,
 - zabrania się ujawniania haseł jakimkolwiek osobom trzecim,
 - zabrania się zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim,
 - zabrania się używania identyfikatora lub hasła innego użytkownika.
4. Prawidłowe wykonywanie obowiązków związanych z korzystaniem użytkowników z haseł nadzoruje administrator bezpieczeństwa informacji. Nadzór ten w szczególności polega na obserwacji (monitorowaniu) funkcjonowania mechanizmu uwierzytelniania i przywracania stanu prawidłowego w przypadku nieprawidłowości.

6. Procedury rozpoczęcia i zakończenia pracy w systemie informatycznym

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych. W przypadku naruszenia ochrony danych osobowych użytkownik niezwłocznie powiadamia administratora danych osobowych.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
 - 1) włączenia komputera,
 - 2) podania hasła dostępu do systemu operacyjnego,
 - 3) uwierzytelnienia się („zalogowania” w programie aplikacyjnym) za pomocą identyfikatora i hasła.
3. Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.

4. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się” z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.

5. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się” lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania” się do systemu.

6. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się” w systemie), użytkownik niezwłocznie powiadamia o nich administratora danych osobowych.

7. Procedury tworzenia kopii archiwalnych i kopii zapasowych

1. Kopie awaryjne tworzone są codziennie automatycznie przez serwery.

2. Kopie archiwalne przechowywane są w archiwum Urzędu Gminy.

3. Sposób, czas przechowywania i sposoby likwidacji nośników informacji, w tym kopii określa instrukcja kancelaryjna.

4. Wydruki i dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w zamkniętych szafach. Okres przechowywania oraz sposób likwidacji tych wydruków określa instrukcja kancelaryjna.

5. Osoba zatrudniona przy przetwarzaniu danych osobowych, sporządzająca wydruk zawierający dane osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności – niezwłocznie wydruk zniszczyć.

6. Fizyczna likwidacja uszkodzonych lub niepotrzebnych elektronicznych nośników informacji z danymi osobowymi odbywa się w sposób uniemożliwiający odczyt danych osobowych, to jest przez formatowanie, złamanie nośnika CD albo rozbicie dysku twardego.

8. Sprawdzanie obecności wirusów komputerowych

1. Sprawdzanie obecności wirusów komputerowych dokonywane jest poprzez zainstalowanie programu antywirusowego, który skanuje automatycznie, bez udziału użytkownika przetwarzane pliki na obecność wirusów. Program jest zainstalowany na wszystkich stacjach roboczych przetwarzających dane osobowe.

2. Po każdej naprawie i konserwacji komputera należy dokonać sprawdzenia pod kątem występowania wirusów i ponownie zainstalować program antywirusowy.

3. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich. Dane uzyskiwane drogą teletransmisji należy umieszczać – przed otwarciem – w katalogu przejściowym, który podlega sprawdzeniu.

9. Ochrona przed oprogramowaniem mającym na celu nieuprawniony dostęp do danych

1. W celu zabezpieczenia przed działalnością oprogramowania, którego celem jest nieuprawniony dostęp do danych, dostęp do sieci Internet jest zabezpieczony za pomocą routera z wbudowanym Firewallem sprzętowym.

2. Pracownicy odbierający pocztę elektroniczną zostali poinformowani o konieczności usuwania wszelkiej podejrzanej korespondencji, szczególnie zawierającej załączniki z plikami wykonywalnymi.

3. Pracowników obowiązuje zakaz samodzielnego instalowania programów.

4. Zasady przeglądów i konserwacji systemu.

5. Przegląd i konserwacja zbiorów danych dokonywane są poprzez:

- badanie spójności bazy danych,
- uruchamianie zapytań do bazy danych w celu analizy danych,
- przegląd wydruków po wyznaczonych procesach,
- sprawdzanie zgodności danych z dokumentami,
- analiza zgłaszanych uwag użytkowników.

6. Przeglądu i konserwacji dokonuje administrator bezpieczeństwa informacji.

10. Komunikacja w sieci komputerowej

W zakresie korzystania z sieci komputerowej obowiązują następujące zasady:

- 1) pracownicy nie są uprawnieni do instalacji jakiegokolwiek prywatnego oprogramowania bez zgody administratora danych osobowych,
- 2) oprogramowanie na komputerach może być zainstalowane wyłącznie przez administratora bezpieczeństwa informacji. Wszelkie dane zainstalowane na komputerach stanowią własność Urzędu Gminy,
- 3) pracownicy nie mają prawa przekazywać za pośrednictwem sieci komputerowej do stron trzecich jakichkolwiek danych stanowiących własność Urzędu Gminy,
- 4) pracownicy nie mogą podłączać się do sieci zewnętrznej za pośrednictwem modemów. W przypadku takiej konieczności należy poinformować administratora bezpieczeństwa informacji.

11. Obowiązki i odpowiedzialność użytkownika związane z obowiązywaniem instrukcji.

1. Użytkownik systemu jest zobowiązany zapoznać się z treścią niniejszej Instrukcji i potwierdzić to podpisem.
2. Naruszenie przez pracownika niniejszej Instrukcji może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu pracy odpowiedzialność pracownika.

WOJT
Krzysztof Wądołowski