

Wójt Gminy
Radków

Zarządzenie Nr 23 /2014

Wójta Gminy w Radkowie

z dnia 30 czerwca 2014 r.

w sprawie: polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Radkowie.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2013 r., poz. 594 z późn. zm.), art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz §3, 4 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024) zarządzam, co następuje:

§ 1

Ustala się:

1. Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Radkowie, stanowiącą załącznik nr 1,
2. Instrukcję zarządzania systemem informatycznym w Urzędzie Gminy w Radkowie, stanowiącą załącznik nr 2.

§ 2

Wykonanie Zarządzenia powierza się Sekretarzowi Gminy.

§ 3

Traci moc Zarządzenie Nr 40/2013 Wójta Gminy w Radkowie z dnia 27 listopada 2013 r. w sprawie: polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Radkowie.

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.



WÓJTA GMINY
Stanisław Herej

**Polityka Bezpieczeństwa przetwarzania danych osobowych
w Urzędzie Gminy w Radkowie**

**Rozdział I
Postanowienia ogólne**

§ 1

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Radkowie zwana dalej „Polityką”, jest dokumentem, którego celem jest określenie podstawowych reguł dotyczących zapewnienia bezpieczeństwa w zakresie przetwarzania danych osobowych
 - a. w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych,
 - b. w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
2. Urząd Gminy w Radkowie, zwany dalej „Urzędem”, realizując Politykę przestrzega staranności w celu zabezpieczenia bezpieczeństwa danych osobowych poprzez zapewnienie ich poufności, integralności i dostępności, w tym aby dane te były:
 - a. przetwarzane zgodnie z prawem,
 - b. zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane przetwarzaniu niezgodnemu z tymi celami,
 - c. merytorycznie poprawne i adekwatne w stosunku do celów, w jakim są przetwarzane,
 - d. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
3. Polityka obowiązuje wszystkie osoby zatrudnione w Urzędzie mające styczność z przetwarzaniem danych osobowych.
4. Polityka bezpieczeństwa podlega okresowej aktualizacji, która jest realizowana przez Administratora Bezpieczeństwa Informacji.

§ 2

Ileokroć w Polityce jest mowa o:

1. Urzędzie – rozumie się przez to Urząd Gminy w Radkowie.
2. Administratora Danych Osobowych – zwanym dalej Administratorem, należy przez to rozumieć Wójta Gminy Radków.
3. Ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z późn. zmianami.
4. Danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
5. Danych osobowych wrażliwych - rozumie się przez to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, orientację seksualną, dane o stanie zdrowia, kodzie genetycznym, nałogach oraz danych dotyczących skazań, orzeczeń o ukaraniu wydanych w postępowaniu sądowym lub administracyjnym.

6. Zbiornice danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
7. Instrukcji – rozumie się przez to Instrukcję zarządzania systemem informatycznym, która obowiązuje w Urzędzie.
8. Administratorze Bezpieczeństwa Informacji, zwanym dalej ABI – należy rozumieć przez to osobę wyznaczoną przez Administratora Danych Osobowych, która odpowiada za nadzorowanie przestrzegania zasad ochrony przetwarzanych danych osobowych w Urzędzie, w tym w szczególności związanych z przeciwdziałaniem dostępowi do danych osobowych osób nieupoważnionych.
9. Administratorze Systemów Informatycznych, zwanym dalej ASI – należy przez to rozumieć informatyka zatrudnionego w Urzędzie, którego celem działania jest nadzorowanie, kontrolowanie zasad bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.
10. Merytorycznym Administratorze Informacji, zwanym dalej MAI – należy przez to rozumieć kierującego jednostką organizacyjną Urzędu właściwą dla danego zakresu danych osobowych, który jest merytorycznie odpowiedzialny za przetwarzanie danych w określonym zakresie.
11. Użytkownika – należy przez to rozumieć pracownika Urzędu, który posiada upoważnienie wydane przez Administratora Danych Osobowych i dopuszczony jest do przetwarzania danych osobowych wynikających z zakresu czynności wykonywanych w Urzędzie.
12. Identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
13. Hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
14. Przetwarzaniu danych osobowych – należy przez to rozumieć wykonywanie jakichkolwiek operacji na danych osobowych, m.in. takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
15. Odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
 - a. osoby, której dane dotyczą,
 - b. osoby uprawnionej do przetwarzania danych,
 - c. podmiotu, któremu powierzono przetwarzanie danych osobowych w drodze umowy,
 - d. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Rozdział 2

Zasady przetwarzania danych osobowych

§ 3

1. Przetwarzanie danych osobowych dopuszczalne jest tylko wtedy, gdy:
 - a. osoba, której dane dotyczą, wyrazi zgodę, chyba że chodzi o usunięcie jej danych,
 - b. jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa,
 - c. jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
 - d. jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

- e. jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw osoby, której dane dotyczą.
2. Każda z przesłanek wymienionych w ust. 1 jest autonomiczna i może stanowić samodzielną podstawę przetwarzania danych osobowych.
3. Zgoda osoby, której dane osobowe dotyczą jest oświadczeniem woli, którego treścią jest zgoda na przetwarzanie jego danych w określonym celu, zakresie przez określonego administratora. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
4. W przypadku zgody na przetwarzanie danych osobowych wrażliwych, zgoda musi być wyrażona na piśmie.

§ 4

1. W przypadku zbierania danych osobowych od osoby, której dane dotyczą należy zapewnić informację dla tej osoby o:
 - a. nazwie i siedzibie Administratora danych osobowych,
 - b. celu zbierania danych, a w szczególności o znanych lub przewidywanych odbiorcach danych osobowych,
 - c. prawie dostępu do treści swoich danych oraz ich poprawiania,
 - d. dobrowolności lub obowiązku podania danych osobowych, a jeżeli taki obowiązek istnieje o jego podstawie prawnej.
2. Przepisu ust. 1 nie stosuje się jeżeli:
 - a. przepisy innych ustaw zezwalają na przetwarzanie danych osobowych bez ujawniania faktycznego celu ich zbierania,
 - b. osoba, której dane dotyczą, posiada informacje o których mowa w ust. 1.

Rozdział 3

Zarządzanie zbiorami danych osobowych

§ 5

1. ABI prowadzi wykaz zbiorów danych osobowych zwany dalej „wykazem zbiorów”.
2. Każdy zbiór opisany jest w wykazie zbiorów poprzez nazwę oraz nazwę programu zastosowanego do przetwarzania danych osobowych.
3. Zobowiązuje się kierowników jednostek organizacyjnych do informowania ABI o planowaniu utworzenia zbioru danych osobowych.
4. Utworzenie nowego zbioru danych osobowych może być wynikiem:
 - a. realizacji nowego celu,
 - b. zidentyfikowania zbioru, który nie został wpisany do wykazu zbioru,
 - c. przyjęcia zbioru danych osobowych w wyniku zawarcia umowy o przetwarzaniu danych.
5. Tworzenie nowego zbioru w systemie informatycznym może nastąpić tylko po uzgodnieniu z ASI i po akceptacji ABI.
6. W przypadku rejestracji nowego zbioru w rejestrze SIODO wnioski rejestracyjne na platformie e-gido wypełnia ASI przy udziale MAI.
7. Dokumenty związane z rejestracją zbioru danych przechowuje ABI.
8. W przypadku zamiaru przyjęcia zbioru danych osobowych w wyniku zawarcia umowy o powierzeniu przetwarzania danych lub przekazania zbioru do przetwarzania podmiotowi zewnętrznemu MAI, realizujący to zadanie zobowiązany jest niezwłocznie przekazać projekt umowy do ABI w celu jego uzgodnienia.

§ 6

1. Aktualizacji zgłoszeń w rejestrze GODO wymagają następujące sytuacje:
 - a. zmiana podstaw prawnych lub celu przetwarzania danych osobowych,
 - b. zmiana zakresu przetwarzania danych,
 - c. zmiana sposobu zbierania oraz udostępniania danych osobowych.
2. W przypadku konieczności aktualizacji zgłoszenia w rejestrze GODO w związku z sytuacją określoną w pkt. 1, potrzebę w tym zakresie zobowiązany jest zgłosić niezwłocznie MAI do ABI. Do procedury aktualizacji zbioru ma zastosowanie § 5 pkt 5 i 6.

§ 7

1. Działania związane z wyrejestrowaniem zbioru danych z rejestru GODO podejmuje ABI na wniosek MAI.
2. Decyzja GODO o wyrejestrowaniu zbioru danych jest podstawą do wykreślenia zbioru z wykazu zbiorów.
3. W przypadku wykreślenia z wykazu zbioru danych, który do przetwarzania danych wykorzystywał system informatyczny, ASI podejmuje działania w celu zapewnienia fizycznego usunięcia zbioru w formie elektronicznej z uwzględnieniem wymogów przepisów o archiwizacji danych.

Rozdział 4

Opis zdarzeń naruszających ochronę danych osobowych

§ 8

1. Naruszenie ochrony danych osobowych, może być spowodowane:
 - a. niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, skutki powodzi, pożaru itp.,
 - b. niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu,
 - c. umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane lub osób odpowiedzialnych za ich ochronę.
2. Za naruszenie ochrony danych uważa się w szczególności:
 - a. przetwarzanie danych bez właściwego upoważnienia,
 - b. przetwarzanie danych z naruszeniem zasad § 3,
 - c. przetwarzania danych w zbiorach nieujętych w wykazie,
 - d. brak możliwości fizycznego dostępu do danych w wyniku np. zgubionego klucza do pomieszczenia lub mebli biurowych, w których przechowywane są dokumenty,
 - e. nieskuteczne zniszczenie nośników informacji zawierających dane, umożliwiające ponowny ich odczyt przez osoby nieuprawnione,
 - f. próba nielegalnego logowania się do systemu lub włamania,
 - g. zmienione oprogramowanie systemu, stwierdzone przez użytkownika.
3. Zakazuje się przekazywania danych osobowych przez niezabezpieczone łącza telefoniczne.

Rozdział 5

Zasady postępowania w sytuacji naruszenia ochrony danych osobowych

§ 9

1. W przypadku stwierdzenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, użytkownik jest zobowiązany do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz ABI.
2. Użytkownik systemu powinien:
 - a. zabezpieczyć dostęp do pomieszczenia lub urzędnia,
 - b. powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony,
 - c. zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony,
 - d. podjąć stosowne do zaistniałej sytuacji działania, które zapobiegają ewentualnej utracie danych.
3. ABI z przebiegu zdarzenia sporządza raport z naruszenia bezpieczeństwa przetwarzania danych, który przekazuje Administratorowi.
4. Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowania przetwarzania danych wyraża ASI.

Rozdział 6

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

§ 10

1. Zasady użytkowania systemów informatycznych służących do przetwarzania danych w Urzędzie określa instrukcja zarządzania systemem informatycznym.
2. Instrukcja opracowywana jest przez ASI i zatwierdzana przez Administratora.
3. ASI wdraża instrukcję do użytku w Urzędzie.

§ 11

1. Dane osobowe w Urzędzie mogą być przetwarzane tylko przez osoby posiadające upoważnienie do przetwarzania danych, wydane przez Administratora. Upoważnienie określa zakres uprawnień do wykonywania operacji na danych.
2. W Urzędzie prowadzona jest ewidencja osób upoważnionych do przetwarzania danych przez ABI.
3. Ewidencja o której mowa w ust. 2 zawiera:
 - a. numer porządkowy i datę nadania upoważnienia,
 - b. imię i nazwisko użytkownika,
 - c. nazwę komórki organizacyjnej, w której jest zatrudniony,
 - d. zakres uprawnień do przetwarzania danych.

§ 12

1. Upoważnienie do przetwarzania danych dla pracownika Urzędu wydawane jest na wniosek kierownika jednostki organizacyjnej, w której pracownik realizuje zadania. We wniosku określony jest zakres uprawnień do przetwarzania danych.
2. Wzór wniosku o upoważnienie do przetwarzania danych stanowi załącznik nr 1 do Polityki.
3. Wzór upoważnienia do przetwarzania danych stanowi załącznik nr 2 do Polityki.
4. Upoważnienie opracowuje ABI. Administrator może upoważnić ABI do podpisania upoważnień.

5. Upoważnienie do przetwarzania danych rejestrowane jest przez ABI w ewidencji osób upoważnionych do przetwarzania danych.
6. W przypadku upoważnienia do przetwarzania danych w systemie informatycznym informacja ta przekazywana jest również do ASI w celu zarejestrowania użytkownika w systemie. Procedura związana z rejestracją użytkownika w systemie informatycznym określona jest w instrukcji.
7. Upoważnienie wydawane jest w dwóch egzemplarzach, jeden przechowywany jest w aktach osobowych pracowników, drugi u ABI.
8. Upoważnienie dla osoby o której mowa w ust. 1 wydawane jest po podpisaniu przez nią oświadczenia o zobowiązaniu się do zachowania w tajemnicy poznanych danych osobowych oraz informacji związanych z funkcjonowaniem systemu ochrony danych, także po ustaniu realizacji wykonywanych zadań.
9. Wzór oświadczenia stanowi załącznik nr 3 do Polityki.
10. Oświadczenie przechowywane jest u ABI.
11. Nadzór nad przestrzeganiem zasad ochrony danych przez pracownika sprawuje właściwy merytorycznie kierownik jednostki organizacyjnej Urzędu.

§ 13

1. Dane osobowe przetwarzane są w budynku i pomieszczeniach, tworzących obszar przetwarzania danych, który określony jest przez Administratora.
2. Wykaz budynków i pomieszczeń tworzących obszar przetwarzania danych stanowi załącznik nr 4 do Polityki.
3. Przebywanie osób trzecich w pomieszczeniu, w którym są przetwarzane dane jest dopuszczalne w obecności osoby upoważnionej do przetwarzania danych.
4. Pomieszczenia, w których przetwarzane są dane są zamykane na czas nieobecności użytkowników, uniemożliwiając do nich dostęp.

§ 14

1. Dane przetwarzane w systemie informatycznym zabezpiecza się przez wykonanie kopii zapasowych zbiorów danych oraz programów i urządzeń programowych służących do przetwarzania danych.
2. Zasady tworzenia kopii zapasowych oraz ich przechowywanie określa instrukcja.

§ 15

1. Kierownik jednostki organizacyjnej Urzędu odpowiedzialny jest za prowadzenie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane.
2. Codzienna kontrolę bezpieczeństwa przetwarzania danych sprawują użytkownicy systemu.

§ 16

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, przeznaczone do likwidacji – pozbawia się wcześniej zapisu tych danych lub uszkadza się w sposób uniemożliwiający ich odczytanie.
2. W celu zapewnienia nieprzerwanej i bezpiecznej pracy systemów informatycznych prowadzone są okresowe przeglądy i konserwacje, które zapewnia ASI. Zasady prowadzenia przeglądów i konserwacji urządzeń komputerowych, systemów informatycznych oraz zbiorów danych określa instrukcja.
3. W celu zapewnienia ochrony serwerów przed utratą danych w wyniku awarii zasilania stosuje się zasilanie awaryjne UPS.

4. W celu zapewnienia ochrony przed utratą danych stosuje się zasilacze awaryjne UPS przy stacjach roboczych odpowiednio do potrzeb.

§ 17

1. Systemy informatyczne służące do przetwarzania danych muszą być wyposażone w mechanizmy kontroli dostępu.
2. Środki stosowane do uwierzytelniania w systemie informatycznym oraz zarządzanie identyfikatorami i hasłami określa instrukcja.
3. Hasło podlega szczególnej ochronie, zakazuje się użytkownikowi jego udostępniania innym osobom.

§ 18

1. Użytkownicy systemów przetwarzające dane nie mogą instalować oraz uruchamiać żadnych aplikacji, które nie zostały wcześniej dopuszczone do użytkowania w Urzędzie.
2. W Urzędzie systemy, w których przetwarzane są dane muszą być wyposażone w mechanizmy ochrony antywirusowej. Stosownie tych mechanizmów oraz ich skuteczność kontroluje ASI.
3. Zasady ochrony antywirusowej określa instrukcja.

§ 19

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym określa instrukcja.

§ 20

1. Pracownicy zapoznają się z przepisami o ochronie danych osobowych.
2. Pracownik podpisuje oświadczenie o zapoznaniu się z przepisami. Wzór oświadczenia stanowi załącznik nr 5 do Polityki. Oświadczenie sporządzane jest w dwóch egzemplarzach, jeden przechowywany jest w aktach osobowych, drugi u ABI.

Rozdział 7

Przepisy końcowe

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych stanowi załącznik nr 6 do Polityki.
2. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami stanowi załącznik nr 7 do Polityki.
3. W przypadku powierzenia przetwarzania danych osobowych stosuje się wzór umowy, który stanowi załącznik nr 8 do Polityki.

WÓJT GMINY
Stanisław Herej

Urząd Gminy Radków
Radków 99
29-135 Radków

Radków,

U P O W A Ż N I E N I E

Na podstawie art. 7 pkt 4 oraz art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) **upoważniam** zatrudnioną/ego na stanowisku do przetwarzania danych osobowych w zakresie:

Upoważnienie jest ważne w czasie zatrudnienia użytkownika u Administratora lub do zmiany zakresu obowiązków użytkownika, lub do ustania realizacji zadań z których wynika brak przetwarzania danych osobowych w zbiorze lub zakresie określonym upoważnieniem.

Niniejsze upoważnienie może zostać cofnięte w każdym czasie.

Po utracie ważności upoważnienia zobowiązuje ww. osobę do zwrotu upoważnienia Administratorowi Danych Osobowych.

Osoby, które zostały upoważnione do przetwarzania danych osobowych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia (art. 39 ust. 2 ustawy o ochronie danych osobowych). Ww. obowiązek trwa również po ustaniu zatrudnienia w Urzędzie Gminy Radków.

Osoba upoważniona do przetwarzania danych osobowych ponosi odpowiedzialność karną za przetwarzanie danych osobowych niezgodnie z ustawą o ochronie danych osobowych zgodnie z przepisami Rozdziału 8 ww. ustawy.

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do bezwzględnego stosowania przepisów ustawy o ochronie danych osobowych, zapisów Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Radkowie oraz Instrukcji zarządzania systemem informatycznym w Urzędzie Gminy w Radkowie.

.....

Administrator Danych Osobowych

Otrzymałem:

.....

Data i podpis pracownika

Radków

Administrator bezpieczeństwa informacji

w/m

wniosuję o udzielenie

Pani/Panu/**

Upoważnienia do przetwarzania danych osobowych w:

.....

(nazwa jednostki organizacyjnej Urzędu)

Z powodu: / przyjęcia do pracy, przejścia na inne stanowisko, zmiany zakresu czynności/ *

.....

Upoważnienie dotyczy:

Nazwa: /zbioru danych osobowych, zbioru danych osobowych tworzonych doraźnie w celach technicznych, rodzaju spraw związanych z przetwarzaniem danych osobowych poza zbiorem w systemach informatycznych w celach edycji/ *

.....

.....

.....

.....

Zakres uprawnień:

.....

.....

.....

Sposób przetwarzania danych osobowych: papierowy / w systemie informatycznym / *

Miejsce przetwarzania danych osobowych: (adres siedziby, piętro, nr pokoju)

.....

.....

(pieczętka i podpis kierownika jednostki organizacyjnej urzędu)

** właściwe skreślić

* właściwe podkreślić

.....
(imię i nazwisko)

.....
(nazwa właściwej merytorycznie jednostki organizacyjnej Urzędu,
Nazwa komisji, itp.)

OŚWIADCZENIE

Oświadczam, że zobowiązuję się do przestrzegania:

1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r., poz. 926 z późniejszymi zmianami).
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie określenia podstawowych 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)

Jednocześnie w czasie wykonywania swoich zadań zobowiązuje się do:

1. zapewnienia ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Radkowie, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom nieuprawnionym, zabraniam, uszkodzeniem oraz nieuprawnioną modyfikacją lub zniszczeniem,
2. zachowania w tajemnicy, także po ustaniu realizacji zadań poznanych danych osobowych oraz informacji związanych z funkcjonowaniem systemu ochrony danych osobowych,
3. zgłaszania Wójtowi gminy Radków próby lub faktu naruszenia bezpieczeństwa danych osobowych.

.....
(podpis)

Radków, dnia

Wykaz budynków i pomieszczeń tworzących obszar przetwarzania danych

Za obszar przetwarzania danych uznaje się obszar, w którym wykonywane są operacje na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Siedziba Urzędu Gminy Radków – Radków 99, 29-135 Radków.

Przetwarzanie danych osobowych odbywa się w następujących pomieszczeniach biurowych:
nr 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 17, 18, 19, 21, 23.

.....
(imię i nazwisko pracownika)

.....
(stanowisko i nazwa jednostki organizacyjnej Urzędu.)

OŚWIADCZENIE

Oświadczam, że zapoznałam(em) się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuje się do przestrzegania:

1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r., poz. 926 z późniejszymi zmianami).
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie określenia podstawowych 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).
3. Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Radkowie.
4. Instrukcji zarządzania systemem informatycznym w Urzędzie Gminy w Radkowie.

Jednocześnie w czasie wykonywania swoich zadań zobowiązuje się do:

1. zapewnienia ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Radkowie, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom nieuprawnionym, zabraniam, uszkodzeniem oraz nieuprawnioną modyfikacją lub zniszczeniem,
2. zachowania w tajemnicy. Także po ustaniu stosunku pracy, wszelkich informacji dotyczących ochrony fizycznej, technicznej i organizacyjnej danych osobowych, funkcjonowania systemów i urządzeń służących do przetwarzania danych osobowych w Urzędzie Gminy w Radkowie,
3. zachowania w tajemnicy hasła dostępu do systemów informatycznych, przetwarzających dane osobowe w Urzędzie Gminy Radków, również po upływie jego ważności,
4. natychmiastowego zgłaszania przełożonemu i Administratorowi Bezpieczeństwa Informacji stwierdzenia na swoim stanowisku pracy próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa danych osobowych lub systemu informatycznego, w którym przetwarzane są dane osobowe

.....
(podpis)

Radków, dnia

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

Lp.	Nazwa zbioru danych	Nazwa programu zastosowanego do przetwarzania danych osobowych
1.	Ewidencja Ludności i dowodów osobistych w gminie Radków, woj. świętokrzyskie	PUMA
2.	Zbiór kopert dokumentów stwierdzających tożsamość w gminie Radków, woj. świętokrzyskie	System wydawania dowodów osobistych
3.	Zbiór aktów stanu cywilnego w gminie Radków, woj. świętokrzyskie	PUMA
4.	Podatek od środków transportu w gminie Radków, woj. świętokrzyskie	ewidencja wyłącznie papierowa
5.	Podatki i opłaty lokalne w gminie Radków, woj. świętokrzyskie	PUMA
6.	Gminna Biblioteka Publiczna w gminie Radków, woj. Świętokrzyskie	ewidencja wyłącznie papierowa
7.	Zbiór danych dotyczących opieki społecznej w gminie Radków, woj. Świętokrzyskie	POMOST, ŚWIADCZENIA RODZINNE I FUNDUSZ ALIMENTACYJNY.
8.	Kwalifikacja wojskowa	Program SELWIN
9.	Awanse zawodowe nauczycieli	Wersja papierowa
10.	Właściciele psów agresywnych	Wersja papierowa
11.	Ewidencja tytułów wykonawczych	Program PUMA
12.	Ewidencja miejscowości, ulic i adresów	Program UMUiA
13.	Lokale komunalne	Program PUMA
14.	Ewidencja szamb	Program Districtus
15.	Zmiana imion i nazwisk	Wersja papierowa
16.	Świadczenia osobiste i rzeczowe	Wersja papierowa
17.	Ewidencja zezwoleń na sprzedaż napojów alkoholowych	Program PUMA
18.	Zamówienia publiczne	Wersja papierowa
19.	Skargi i wnioski	Wersja papierowa
20.	Oświadczenia majątkowe wójta, sekretarza, skarbnika, kierowników gminnych jednostek organizacyjnych	Wersja papierowa
21.	Oświadczenia majątkowe - radnych	Wersja papierowa
22.	Wnioski o udostępnianie informacji	Wersja papierowa

	publicznej	
23.	Wycinka drzew	Wersja papierowa
24.	Ochotnicza Straż Pożarna	Wersja papierowa
25.	Postępowanie sprawdzające	Wersja papierowa
26.	Zagospodarowanie przestrzenne	Wersja papierowa
27.	Rejestr decyzji rozgraniczających	Wersja papierowa
28.	Podział nieruchomości	Wersja papierowa
29.	Kontrahenci Urzędu Gminy	Program PUMA
30.	Zakładowy Fundusz Świadczeń Socjalnych	Program PUMA
31.	Kasa Zapomogowo-Pożyczkowa	Program PUMA
32.	Sprzedaż nieruchomości gminnych	Program PUMA
33.	Decyzje środowiskowe	Wersja papierowa
34.	Skazani na prace społeczne	Wersja papierowa
35.	Zwrot podatku akcyzowego	Program PUMA
36.	Utylizacja azbestu	Wersja papierowa
37.	Opłaty śmieciowe	Wersja papierowa
38.	Ewidencja wydanych pozwoleń na korzystanie z przystanków autobusowych na terenie gminy	Wersja papierowa
39.	Pracownicy Urzędu Gminy	Program PUMA
40.	Kandydaci do pracy	Wersja papierowa

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami

- 1) w zbiorze danych „Ewidencja ludności i dowodów osobistych w Gminie Radków Województwo Świętokrzyskie” przetwarzane są dane osobowe w zakresie:
 - a) nazwiska i imiona,
 - b) imiona rodziców,
 - c) data urodzenia,
 - d) miejsce urodzenia,
 - e) adres zamieszkania lub pobytu,
 - f) numer ewidencyjny PESEL,
 - g) miejsce pracy,
 - h) zawód,
 - i) wykształcenie,
 - j) seria i numer dowodu osobistego,
 - k) nazwisko rodowe matki, ojca,
 - l) stan cywilny,
 - m) data zawarcia małżeństwa,
 - n) numer aktu małżeństwa,
 - o) adres pobytu czasowego,
 - p) seria i numer książeczki wojskowej,
 - q) nazwiska i imiona poprzednie,
 - r) płeć,
 - s) data i numer aktu urodzenia,
 - t) oznaczenie USC,
 - u) obywatelstwo,
 - v) imię i nazwisko rodowe małżonka,
 - w) numery ewidencyjne PESEL: współmałżonka,
 - x) dane odnośnie rozwiązania małżeństwa,
 - y) data i numer aktu: urodzenia, małżeństwa, zgonu,
 - z) numer aktu zgonu,
 - aa) informacje meldunkowe,
 - bb) imię i nazwisko współmałżonka, obecne i poprzednie,
 - cc) informacje dotyczące powszechnego obowiązku obrony RP,
 - dd) stosunek do powszechnego obowiązku obrony (stopień wojskowy, numer i wystawca wojskowego dokumentu tożsamości, przynależność do właściwej wojskowej komendy uzupełnień),
 - ee) informacje dotyczące poprzednio wydanych dowodów osobistych,
 - ff) informacje o prawie osiedlenia się i pobytu,
 - gg) dane o osobach posiadających status uchodźcy,
 - hh) dokumenty związane z przyznaniem statusu uchodźcy,
 - ii) informacje dotyczące pobytu obywateli UE, zezwolenia na pobyt rezydenta długoterminowego,
 - jj) dane dotyczące innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;
- 2) w zbiorze danych „Gminna Biblioteka Publiczna w Gminie Radków Województwo Świętokrzyskie” przetwarzane są dane osobowe w zakresie:
 - a) nazwiska i imiona,
 - b) imiona rodziców,
 - c) data urodzenia,
 - d) adres zamieszkania lub pobytu,
 - e) miejsce pracy,
 - f) zawód,

g) seria i numer dowodu osobistego,

Inne dane osobowe:

Dla osób uczących się można podać szkołę zamiast miejsca pracy oraz dane o legitymacji szkolnej zamiast dowodu osobistego

- 3) w zbiorze danych „Zbiór kopert dokumentów stwierdzających tożsamość w Gminie Radków Województwo Świętokrzyskie” przetwarzane są dane osobowe w zakresie:
 - a) nazwiska i imiona,
 - b) imiona rodziców,
 - c) data urodzenia,
 - d) miejsce urodzenia,
 - e) adres zamieszkania lub pobytu,
 - f) numer ewidencyjny PESEL,
 - g) zawód,
 - h) wykształcenie,
 - i) seria i numer dowodu osobistego,
 - j) stan cywilny,
 - k) rysopis,
 - l) wizerunek;
- 4) w zbiorze danych „Podatek od środków transportowych w Gminie Radków Województwo Świętokrzyskie” przetwarzane są dane osobowe w zakresie:
 - a) nazwiska i imiona,
 - b) adres zamieszkania lub pobytu,
 - c) numer rejestracyjny pojazdu,
 - d) numer NIP;
- 5) w zbiorze danych „Podatki i opłaty lokalne w Gminie Radków Województwo Świętokrzyskie” przetwarzane są dane osobowe w zakresie:
 - a) nazwiska i imiona,
 - b) imiona rodziców,
 - c) adres zamieszkania lub pobytu,
 - d) numer ewidencyjny PESEL,
 - e) numer NIP;
- 6) w zbiorze danych „Zbiór aktów stanu cywilnego w Gminie Radków Województwo Świętokrzyskie” przetwarzane są dane osobowe w zakresie:
 - a) Nazwiska i imiona
 - b) Imiona rodziców
 - c) Data urodzenia
 - d) Adres zamieszkania lub pobytu
 - e) Numer ewidencyjny PESEL
 - f) Zawód
 - g) Wykształcenie
 - h) Seria i numer dowodu osobistego

Inne dane osobowe: płeć, nazwisko rodowe, nazwisko z poprzedniego małżeństwa, stan cywilny, miejsce urodzenia, data zawarcia małżeństwa, miejsce zawarcia małżeństwa, nazwisko po zawarciu małżeństwa, nazwisko ojca, imiona ojca, nazwisko rodowe ojca, data urodzenia ojca, miejsce urodzenia ojca, miejsce zameldowania ojca w chwili urodzenia dziecka, nazwisko matki, imiona matki, nazwisko rodowe matki, data urodzenia matki, miejsce urodzenia matki, miejsce zameldowania matki w chwili urodzenia dziecka, data zgonu, godzina zgonu, miejsce zgonu, data znalezienia zwłok, godzina znalezienia zwłok, miejsce znalezienia zwłok, orzeczenia sądowe dotyczące rozwodu, uznania bądź zaprzeczenia ojcostwa, unieważnienia aktów stanu cywilnego.

- 7) w zbiorze danych „Zbiór danych dotyczących opieki społecznej w Gminie Radków Województwo Świętokrzyskie” przetwarzane są dane osobowe w zakresie:
 1. Nazwiska i imiona
 2. Imiona rodziców
 3. Data urodzenia

4. Miejsce pracy
5. Zawód
6. Wykształcenie
7. Adres zameldowania i zamieszkania
8. Numer ewidencyjny PESEL
9. Seria i numer dowodu osobistego

Inne dane osobowe: płeć, stan cywilny, stan zdrowia, źródła utrzymania, wysokość dochodu, przyczyna udzielenia pomocy (ubóstwo, sieroctwo, bezdomność, potrzeba ochrony macierzyństwa, bezrobociem niepełnosprawność, długotrwała choroba, niezaradność w sprawach opiekuńczo-wychowawczych i prowadzeniu gospodarstwa domowego, rodzina niepełna, wielodzietna, alkoholizm, narkomania, trudność w przystosowaniu się do życia po opuszczeniu zakładu karnego, klęska żywiołowa lub ekologiczna, zdarzenie losowe)

- sytuacja osób niepełnosprawnych: grupa inwalidzka, rodzaj schorzenia, data i numer orzeczenia o niepełnosprawności, termin kolejnego badania, wynik orzeczenia o niepełnosprawności, przyczyna i stopień niepełnosprawności, rodzaj dysfunkcji, ograniczenia funkcjonowania, niezbędny sprzęt ortopedyczny i środki pomocnicze,
 - sytuacja osób z zaburzeniami psychicznymi: grupa inwalidzka, rodzaj schorzenia, data i numer orzeczenia o niepełnosprawności, termin kolejnego badania, wynik orzeczenia o niepełnosprawności, stopień samodzielności osoby chorej psychicznie lub umysłowo upośledzonej, czy osoba jest poddana leczeniu w szpitalu lub przychodni specjalistycznej, czy osoba jest lub była kiedykolwiek leczona przez psychiatrę, wskazania do korzystania z usług specjalistycznych,
 - sytuacja osób uzależnionych: rodzaj uzależnienia, czy osoba uzależniona wyraża zgodę na podjęcie leczenia, jeśli nie to dlaczego, czy podjęto leczenie odwykowe, data podjęcia leczenia odwykowego, wynik leczenia odwykowego.
- 8) w zbiorze danych „Kwalifikacja wojskowa” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) PESEL,
 - d) nazwisko rodowe,
 - e) miejsce urodzenia,
 - f) nr dowodu osobistego;
 - 9) w zbiorze danych „Awanse zawodowe nauczycieli” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) data urodzenia,
 - d) miejsce urodzenia,
 - e) nazwisko rodowe,
 - f) wykształcenie,
 - g) przygotowania pedagogiczne,
 - h) wymiar zatrudnienia,
 - i) nr telefonu,
 - j) stopień awansu zawodowego;
 - 10) w zbiorze danych „Właściciele psów agresywnych” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania;
 - 11) w zbiorze danych „Ewidencja tytułów wykonawczych” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania;
 - 12) w zbiorze danych „Ewidencja miejscowości, ulic i adresów” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania;

- 13) w zbiorze danych „Lokale komunalne” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania;
- 14) w zbiorze danych „Ewidencja szamb” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania;
- 15) w zbiorze danych „Zmiana imion i nazwisk” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) PESEL,
 - d) nr dowodu osobistego;
- 16) w zbiorze danych „Świadczenia osobiste i rzeczowe” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) nr rejestracyjny pojazdu;
- 17) w zbiorze danych „Ewidencja zezwoleń na sprzedaż napojów alkoholowych” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres punktu sprzedaży,
 - c) NIP;
- 18) w zbiorze danych „Zamówienia publiczne” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) NIP,
 - d) REGON,
 - e) numer telefonu;
- 19) w zbiorze danych „Skargi i wnioski” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) adres zamieszkania;
- 20) w zbiorze danych „Oświadczenia majątkowe wójta, sekretarza, skarbnika, kierowników gminnych jednostek organizacyjnych” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) data urodzenia,
 - c) miejsce urodzenia,
 - d) nazwisko rodowe,
 - e) miejsce pracy,
 - f) zasoby pieniężne,
 - g) zobowiązania,
 - h) wysokość dochodów,
 - i) składniki mienia nieruchomości i ruchomego,
 - j) miejsce zamieszkania i położenia nieruchomości,
 - k) PESEL,
 - l) NIP;
- 21) w zbiorze danych „Oświadczenia majątkowe radnych” przetwarzane są dane osobowe w zakresie:
 - a) imię i nazwisko,
 - b) data urodzenia,
 - c) miejsce urodzenia,
 - d) nazwisko rodowe,
 - e) miejsce pracy,
 - f) zasoby pieniężne,
 - g) zobowiązania,
 - h) wysokość dochodów,
 - i) składniki mienia nieruchomości i ruchomego,
 - j) miejsce zamieszkania i położenia nieruchomości,
 - k) PESEL,
 - l) NIP;
- 22) w zbiorze danych „Wnioski o udostępnianie informacji publicznej” przetwarzane są dane osobowe w zakresie:

- a) imię i nazwisko,
 - b) adres e-mail,
 - c) numer telefonu;
- 23) w zbiorze danych „Wycinka drzew” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) numer działki,
 - d) numer telefonu;
- 24) w zbiorze danych „Ochotnicza Straż Pożarna” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) PESEL,
 - d) NIP,
 - e) nr telefonu,
 - f) nr prawa jazdy;
- 25) w zbiorze danych „Postępowanie sprawdzające” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) data i miejsce urodzenia,
 - c) imiona rodziców,
 - d) nr dowodu osobistego,
 - e) PESEL,
 - f) NIP,
 - g) seria i nr książeczki wojskowej,
 - h) stopień wojskowy,
 - i) adres zamieszkania,
 - j) miejsce pracy,
 - k) stanowisko,
 - l) wysokość przychodów,
 - m) daty urodzenia rodziców i miejsce,
 - n) daty urodzenia rodzeństwa i miejsce,
 - o) adresy zamieszkania rodzeństwa, miejsca ich pracy,
 - p) imiona dzieci, ich daty i miejsce urodzenia, adresy zamieszkania, miejsca pracy;
- 26) w zbiorze danych „Zagospodarowanie przestrzenne” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) nr działki;
- 27) w zbiorze danych „Rejestr decyzji rozgraniczających” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) nr działki;
- 28) w zbiorze danych „Podział nieruchomości” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) nr działki;
- 29) w zbiorze danych „Kontrahenci Urzędu Gminy” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) PESEL,
 - d) NIP;
- 30) w zbiorze danych „Zakładowy Fundusz Świadczeń Socjalnych” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) wysokość dochodów;
- 31) w zbiorze danych „Kasa zapomogowo-pożyczkowa” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) miejsce pracy;
- 32) w zbiorze danych „Sprzedaż nieruchomości gminnych” przetwarzane są dane osobowe w

- zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) nr telefonu,
 - d) PESEL,
 - e) NIP;
- 33) w zbiorze danych „Decyzje środowiskowe” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania;
- 34) w zbiorze danych „Skazani na prace społeczne” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) imię ojca,
 - d) data i miejsce urodzenia,
 - e) wymiar kary;
- 35) w zbiorze danych „Zwrot podatku akcyzowego” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) nr rachunku bankowego,
 - d) PESEL;
- 36) w zbiorze danych „Utylizacja azbestu” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) nr telefonu,
 - d) nr działki,
 - e) NIP;
- 37) w zbiorze danych „Opłaty śmieciowe” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) PESEL,
 - d) numer telefonu;
- 38) w zbiorze danych „Ewidencja wydanych pozwoleń na korzystanie z przystanków autobusowych na terenie gminy” przetwarzane są dane osobowe w zakresie:
- a) imię i nazwisko,
 - b) adres zamieszkania,
 - c) NIP;
- 39) w zbiorze danych „Pracownicy Urzędu Gminy” przetwarzane są dane osobowe w zakresie:
- a) Imię i nazwisko,
 - b) adres zamieszkania,
 - c) data i miejsce urodzenia,
 - d) imiona rodziców,
 - e) stan cywilny,
 - f) stan rodzinny,
 - g) wykształcenie,
 - h) NIP,
 - i) PESEL,
 - j) seria i nr dowodu osobistego,
- 40) w zbiorze danych „Kandydaci do pracy” przetwarzane są dane osobowe w zakresie:
- a) Imię i nazwisko,
 - b) adres zamieszkania,
 - c) wykształcenie,
 - d) obywatelstwo,
 - e) data i miejsce urodzenia,
 - f) imiona rodziców,
 - g) NIP,
 - h) PESEL,
 - i) seria i nr dowodu osobistego,
 - j) nr telefonu.

Szczegółowy opis struktury zbiorów danych osobowych wraz ze wskazaniem poszczególnych pól informacyjnych i powiązań między nimi został przygotowany na podstawie materiałów dostarczonych przez twórców oprogramowania służącego do przetwarzania danych osobowych. Ponadto ww. opis struktury wraz ze wskazaniem poszczególnych pól informacyjnych i powiązań między nimi znajduje się w dokumentacji technicznej dostarczonej przez autorów oprogramowania.

Przepływ danych pomiędzy systemami odbywa się w:

System „A”	System „B”	Uwagi	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Program PUMA	Płatnik	Przekazywane są dane dotyczące składek na ubezpieczenia	Jednokierunkowo z programu „A” do Programu „B”	Automatycznie

Sposób przepływu danych między poszczególnymi systemami znajduje się w dokumentacji technicznej dostarczonej przez autorów oprogramowania.

Wzór umowy powierzenia przetwarzania danych osobowych

zawarta w Radkowie w dniu r. pomiędzy:

Urzędem Gminy w Radkowie z siedzibą przy ul.
reprezentowaną/ym przez:, zwaną/ym dalej Zleceniodawcą
(Administratorem Danych Osobowych),

a

..... z siedzibą w zarejestrowaną/ym
w pod numerem, posiadającą/ym numer NIP
..... oraz numer REGON, reprezentowaną/ym przez:
....., zwaną/ym dalej Procesorem

§ 1.

Definicje

1. Procesor – podmiot, któremu powierzono przetwarzanie danych osobowych na mocy umowy powierzenia ze Zleceniodawcą,
2. Administrator Danych Osobowych - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych,
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. 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,
5. Ustawa - Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926, z późn. zm.),
6. 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 (Dz. U. Nr 100, poz. 1024),
7. GIODO – Generalny Inspektor Ochrony Danych Osobowych

§ 2.

Przedmiot Umowy

1. **Przedmiotem** umowy jest powierzenie Procesorowi przez Administratora Danych Osobowych przetwarzania danych osobowych ze zbioru danych osobowych o nazwie:
2. **Celem** przetwarzania powierzonego zbioru danych osobowych jest
3. **Zakres** przetwarzania obejmuje następujące dane osobowe:

§ 3.

Zobowiązania Procesora i Zleceniodawcy

1. Procesor zobowiązuje się przetwarzać powierzone dane wyłącznie w zakresie i celu przewidzianym w Umowie.
2. Procesor zobowiązuje się przed przystąpieniem do przetwarzania danych powierzonych przez Zleceniodawcę wdrożyć i utrzymywać przez czas przetwarzania wszelkie środki techniczne i organizacyjne, przewidziane w art. 36-39 Ustawy.
3. Procesor zobowiązuje się przed przystąpieniem do przetwarzania danych powierzonych przez Zleceniodawcę spełnić wymagania określone w przepisach, o których mowa w art. 39a Ustawy.

§ 4.

Szczegółowe zobowiązania Procesora dla powierzonych danych osobowych, wynikające z realizacji wymagań art. 36-39a Ustawy

1. Procesor oświadcza, że do nadzoru nad przestrzeganiem zasad ochrony, o których mowa w § 3 ust. 2 wyznacza Administratora Bezpieczeństwa Informacji.
2. Procesor zobowiązuje się do dopuszczania do przetwarzania danych wyłącznie osoby posiadające upoważnienie nadane przez Procesora, zgodnie z następującymi punktami:
 - a) Procesor przeprowadza szkolenie z zasad ochrony danych osobowych
 - b) Procesor nadaje upoważnienia pracownikom przeznaczonym do przetwarzania danych osobowych w ramach realizacji warunków Umowy.
3. Procesor zobowiązuje się do zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
4. Procesor zobowiązuje się do prowadzenia ewidencji osób upoważnionych do ich przetwarzania.
5. Procesor zobowiązuje się do zapewnienia, że osoby, które zostały przez niego upoważnione do przetwarzania danych, będą zachowywały w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia. Obowiązek ten będzie trwał także po ustaniu zatrudnienia.
6. Procesor oświadcza, że opracował i wdrożył Politykę bezpieczeństwa oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zgodnie z wymaganiami Rozporządzenia.

§ 5.

Dodatkowe zobowiązania Procesora wynikające z realizacji wymagań art. 36-39a Ustawy

1. Procesor nie może powierzyć wykonania wszystkich lub choćby części czynności Umowy innemu podmiotowi (Podprocesorowi) bez uprzedniej pisemnej zgody Administratora Danych Osobowych
2. Po rozwiązaniu lub wygaśnięciu Umowy Procesor zobowiązuje się niezwłocznie zwrócić Zleceniodawcy powierzone zbiory danych i trwale usunąć je z wszystkich nośników, zarówno w wersji elektronicznej jak i papierowej. Zobowiązanie o którym mowa w ust. 2 obejmuje również te podmioty, które przetwarzają dane na zlecenie Procesora, jako Podprocesorzy.
3. Procesor zobowiązuje się w ciągu 7 dni od daty usunięcia danych przekazać Zleceniodawcy protokoły zniszczenia zbiorów danych osobowych.
4. Zleceniodawca zastrzega możliwość przeprowadzenia kontroli Procesora w zakresie przestrzegania wymagań art. 36-39a Ustawy. Kontrola taka może się odbywać w godzinach pracy po uprzednim powiadomieniu Procesora.
5. Po kontroli Zleceniodawca może przekazać Procesorowi pisemne zalecenia pokontrolne wraz z terminem ich realizacji.
6. Procesor zobowiązuje się do niezwłocznego poinformowania Zleceniodawcy o jakimkolwiek postępowaniu administracyjnym lub sądowym, decyzji administracyjnej, orzeczeniu, zapowiadanych kontrolach i inspekcjach, jeśli dotyczą one danych osobowych powierzonych przez Zleceniodawcę.

§ 6.

Odpowiedzialności i kary

1. Procesor przyjmuje do wiadomości, iż podczas realizacji Umowy w zakresie przestrzegania przepisów art. 36-39a Ustawy, ponosi odpowiedzialność jak Zleceniodawca.
2. Procesor przyjmuje do wiadomości, iż w związku z realizacją Umowy może być poddany kontroli zgodności przetwarzania danych przez GIODO, z zastosowaniem odpowiednio przepisów art. 14 – 19 Ustawy.
3. Procesor odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały w związku z nienależytym przetwarzaniem przez niego powierzonych danych osobowych.
4. W przypadku naruszenia przepisów Ustawy w ramach realizacji Umowy z przyczyn leżących po stronie Procesora, w następstwie którego Zleceniodawca zostanie zobowiązany do wypłaty odszkodowania lub ukarany grzywną, prawomocnym wyrokiem lub decyzją właściwego organu, Procesor zobowiązuje się do zwrócenia równowartości odszkodowania lub grzywny poniesionych przez Zleceniodawcę.

§ 7.

Obowiązywanie umowy

1. Umowa zostaje zawarta na czas określony do dnia r.
2. Zleceniodawca może wypowiedzieć Umowę ze skutkiem natychmiastowym, w przypadku:
 - a) rażącego naruszenia przez Procesora postanowień Umowy,

b) wyrządzenia przez Procesora przy wykonaniu Umowy szkody Zleceniodawcy lub osobie, której dane Procesor przetwarza na mocy umowy powierzenia,

c) wszczęcia przez GIODO postępowania przeciw Procesorowi w związku z naruszeniem zasad ochrony danych osobowych, jeśli postępowanie dotyczy danych osobowych powierzonych przez Zleceniodawcę.

§ 8.

Postanowienia końcowe

1. Wszelkie zmiany Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych Umową, zastosowanie znajdują przepisy polskiego prawa, w tym Ustawy oraz Kodeksu Cywilnego.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....

Zleceniodawca

.....

Procesor

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W URZĘDZIE GMINY W RADKOWIE

Podstawa prawna: 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) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

Rozdział 1

Definicje

Ilekcroć w niniejszym dokumencie jest mowa o:

1. Urzędzie – należy przez to rozumieć Urząd Gminy w Radkowie.
2. Administratorze Danych – należy przez to rozumieć Wójta Gminy Radków.
3. Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony danych osobowych, ustanowionej zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu.
4. Administratorze systemów Informatycznych – należy przez to rozumieć informatyka zatrudnionego w Urzędzie.
5. Użytkownika systemu – należy przez to rozumieć pracownika upoważnionego do przetwarzania danych osobowych w systemie informatycznym Urzędu.
6. Sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych jej potrzeb, przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
7. Sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. _ Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.).

Rozdział 2

Procedury nadawania i zmiany uprawnień do przetwarzania danych

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
Polityką bezpieczeństwa dotyczącą przetwarzania danych osobowych w Urzędzie Gminy w Radkowie.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 5 do polityki bezpieczeństwa.
3. Administrator systemów informatycznych przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) Administratora Danych określającego zakres uprawnień pracownika, którego wzór stanowi załącznik nr 1 do niniejszej instrukcji.
4. Jedynie prawidłowo wypełniony wniosek o nadanie uprawnień w systemie oraz zmianę tych uprawnień jest podstawą rejestracji uprawnień w systemie.
5. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
6. Hasło ustanowione podczas przyznawania uprawnień przez Administratora systemów informatycznych należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym. Ustanowione hasło, administrator przekazuje użytkownikowi ustnie.
7. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
8. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

9. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
10. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
11. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
12. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
13. Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
14. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora systemów informatycznych o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
15. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować w systemie informatycznym, w którym są one przetwarzane oraz unieważnić jej hasło.
16. Administrator systemów informatycznych zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich identyfikatorów w systemie informatycznym.
17. Rejestr, którego wzór stanowi załącznik nr 2, powinien zawierać:
 - imię i nazwisko użytkownika systemów informatycznych,
 - identyfikator,
 - datę nadania uprawnienia,
 - datę odebrania uprawnienia,
 - przyczynę odebrania uprawnienia.
18. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

Rozdział 3

Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz na dwa miesiące.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Pracownik nie ma prawa do udostępniania haseł danej grupy osobom spoza tej grupy, dla której zostały one utworzone.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
9. Przy wyborze hasła obowiązują następujące zasady:
 - a. Minimalna długość hasła – 8 znaków,
 - b. Zakazuje się stosować:
 - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
 - swojej nazwy użytkownika w jakiegokolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.),
 - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.
 - wyrazów słownikowych,
 - przewidywalnych sekwencji znaków z klawiatury np.: „QWERTY”, „12345678”, itp.,
 - c. należy stosować:
 - hasła zawierające kombinacje liter i cyfr,
 - hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole: @, #, itp., o ile system informatyczny na to pozwala,

- hasła, które można zapamiętać bez zapisywania.
10. Zmiany hasła nie wolno zlecać innym osobom.
 11. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

Rozdział 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania się z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputera innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania się z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wylogować się z sieci komputerowej.
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

Rozdział 5

Procedury tworzenia zabezpieczeń

1. Na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się wysoki poziom zabezpieczeń.
2. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego, w przypadku jego nieobecności inna wyznaczona osoba.
3. Pełne kopie bezpieczeństwa serwerów wykonywane są codziennie i zapisywane na osobnych dyskach USB lub dyskach sieciowych przy pomocy programów służących do wykonywania kopii zapasowych.
4. Zabezpieczenie danych znajdujących się na stacjach roboczych wykonywane jest przez program do kopiowania danych zainstalowanych na stacji roboczej. Dane kopiowane są na dysk sieciowy i kompresowane.

Rozdział 6

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji, zawierających dane osobowe oraz wydruków

A. Elektroniczne nośniki informacji

1. Dane osobowe w postaci elektronicznej – za wyjątkiem kopii bezpieczeństwa – zapisane na płytach, pendrivach, dyskach USB czy dyskach twardych nie są wynoszone poza siedzibę Urzędu.
2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych Urzędu.
3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamkniętych szafach biurowych lub kasetkach.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

B. Wydruki

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe, należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

Rozdział 7

Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

1. Na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe, antyspamowe, pracujące w trybie monitora.
2. Każda poczta e-mail przychodząca do Urzędu musi być sprawdzona pod kątem występowania wirusów, spamu.
3. Definicje wzorców wirusów muszą być aktualizowane codziennie.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania i Internetu plików niewiadomego pochodzenia, w szczególności instalowania i użytkowania oprogramowania typu P2P. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
7. Administrator Systemu Informatycznego przeprowadza cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum co miesiąc.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie wymienne nośniki posiadane przez użytkownika. Sprawdzana jest także cała sieć Urzędu.

Rozdział 8

Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnianie danych osobowych, w jakiegokolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnianie danych osobowych nie może być realizowane drogą telefoniczną.
4. Udostępnianie danych osobowych może nastąpić wyłącznie po przedstawieniu wniosku.
5. Kierownicy komórek organizacyjnych prowadzą rejestry udostępnionych danych osobowych zawierające co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję dla której dane udostępniono.

Rozdział 9

Sposób postępowania w sytuacji naruszenia ochrony danych osobowych

1. Sposób postępowania w sytuacji stwierdzenia naruszenia ochrony danych osobowych określa Rozdział 5 Polityki.

Rozdział 10

Procedury wykonywania przeglądów i konserwacji systemu

A. Przeglądy i konserwacja urządzeń

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.
2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.
3. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

B. Przegląd programów i narzędzi programowych

1. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
2. Wszystkie logi opisujące pracę systemu, logowanie użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na nośniku wymiennym.

Rozdział 11

Połączenie do sieci Internet

Połączenie lokalnej sieci komputerowej Urzędu z Internetem jest dopuszczalne wyłącznie po zainstalowaniu kompleksowego oprogramowania antywirusowego.

WÓJT GMINY

~~Stanisław~~ Herej

Radków,

.....
(imię i nazwisko)

.....
(stanowisko)

.....
(wydział)

Wniosek o rejestrację w systemie informatycznym

Proszę o rejestrację w/w pracownika w następującym systemie informatycznym:

.....
.....

Zakres uprawnień w systemie:.....
.....

Data uruchomienia konta w systemie:

.....
(podpis przełożonego)

.....
(podpis pracownika)

Wyrażam zgodę / Nie wyrażam zgody

.....
(podpis Administratora Danych)

Nadano identyfikator:

.....
(podpis ABI)