Wójt Gminy
Radków

128

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.

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

Zarządzenie wchodzi w życie z dniem podjęcia.

GMINA RADKÓW

WÓJT GMINY
Stanisław Herej

Wójt Gminy
Radków

Załącznik nr 1
do Zarządzenia Nr 40/2013
Wójta Gminy w Radkowie
z dnia 27 listopada 2013 r.

125

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

Ilekroć 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. Zbiorze 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 zarzadzania systemem informatycznym, która obowiązuje w Urzędzie.
8. Administratorze Bezpieczeństwa Informacji, zwanym dalej ABI – należy rozumieć przez to osobę wyznaczona 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 przetwarzani 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. Użytkowniku – 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. Haśle – 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 wniosek rejestracyjny na platformie e-giodo 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 GIODO 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 GIODO 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 GIODO podejmuje ABI na wniosek MAI.
2. Decyzja GIODO 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 urządzenia,
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 utrata 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 zarzadzanie 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 musza 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 pracodawcy przez ABI.
2. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi stanowi załącznik nr 7 do Polityki pracodawcy przez ABI.

WÓJT GMINY
Stanisław Herej

Załącznik Nr 1 do „Polityki" 136

Radków .....

Administrator bezpieczeństwa informacji

w/m

wnioskuję 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)

.....

.....

(pieczątka i podpis kierownika jednostki organizacyjnej urzędu)

** właściwe skreślić

* właściwe podkreślić

Załącznik Nr 2 do „Polityki"

Radków, dnia .....

UPOWAŻNIENIE

Nr .....

na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r o ochronie danych Osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami)

Upoważniam

Panią/ Pana *.....

do przetwarzania danych osobowych

W ramach .....
(nazwa zbioru danych osobowych, nazwa zbioru tworzonego doraźnie do celów technicznych, nazwa rodzaju spraw związanych z przetwarzaniem danych osobowych poza zbiorem w systemach informatycznych w celu edycji/**)

Przetwarzanie danych osobowych może odbywać się przy wykorzystaniu: .....

.....
(systemu informatycznego, systemu w postaci papierowej)

w zakresie .....

.....
(nazwa uprawnień w zakresie przetwarzania danych)

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.

.....
(Administrator Danych Osobowych)

---

* niepotrzebne 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, zabraniem, 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

Lp.	Nr pokoju	Określenie w strukturze organizacyjnej urzędu
Budynek Urzędu Gminy w Radkowie – Radków 99		
1.	19	Referat Spraw Obywatelskich Obronnych i Obrony cywilnej
2.	19	USC
3.	11	Referat finansowo-budżetowy
4.	6, 7 i 8	Gminny Ośrodek Pomocy społecznej
5.	-	Gminna Biblioteka Publiczna

.....
(imię i nazwisko pracownika)

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

OŚWIADCZENIE

Oświadczam, że zapoznałam(em) się z przepisami dotyczącymi ochrony danych osobowych i 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).
3. Polityki bezpieczeństwa dotyczącej sposobu przetwarzania danych osobowych w Urzędzie Gminy w Radkowie.
4. Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych 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, zabraniem, 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 .....

Załącznik nr 6 do „Polityki"

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.

Opis struktury zbiorów danych

Ewidencja ludności i dowodów osobistych, zbiór kopert dokumentów stwierdzających tożsamość:

1. Nazwiska i imiona
2. Imiona rodziców
3. Data urodzenia
4. Adres zameldowania
5. Numer ewidencyjny PESEL
6. Seria i numer dowodu osobistego
7. Miejsce urodzenia
8. Nazwisko rodowe
9. Nazwisko rodowe rodziców
10. Wzrost
11. Kolor oczu
12. Płeć
13. Fotografia
14. Podpis
15. Nr i seria poprzednich dowodów osobistych

USC:

1. Nazwiska i imiona
2. Imiona rodziców
3. Data urodzenia
4. Adres zameldowania
5. Numer ewidencyjny PESEL
6. Seria i numer dowodu osobistego

Inne dane osobowe: płeć, nazwisko rodowe, 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.

Podatki i opłaty lokalne

1. Nazwiska i imiona
2. Imiona rodziców
3. Adres zameldowania
4. Numer ewidencyjny PESEL
5. Numer identyfikacyjny NIP

Podatek od środków transportowych

1. Nazwiska i imiona
2. Adres zameldowania
3. Numer rejestracyjny pojazdu
4. Numer identyfikacyjny NIP

Gminna Biblioteka Publiczna:

1. Nazwiska i imiona
2. Imiona rodziców
3. Data urodzenia
4. Adres zameldowania
5. Miejsce pracy
6. Zawód
7. Seria i nr dowodu osobistego

Inne dane osobowe:

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

Gminny Ośrodek Pomocy Społecznej:

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.

Wójt Gminy
Radków

144

Załącznik nr 2
do Zarządzenia Nr 40/2013
Wójta Gminy w Radkowie
z dnia 27 listopada 2013 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU 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

Ilekroć 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, ustanowionego zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu.
4. Administratorze systemów Informatycznych – należy przez to rozumieć informatyka zatrudnionego w Urzędzie.
5. Użytkowniku 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.),
   Polityka 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 Bezpieczeństwa Informacji 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 Bezpieczeństwa Informacji 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 Bezpieczeństwa Informacji 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 Bezpieczeństwa Informacji 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 jakiejkolwiek formę (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 zamykanych 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 systemy 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 cala 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 jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnianie danych osobowych nie może być realizowane droga 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 postepowania 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

145

Załącznik Nr 1 do „Instrukcji"

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)