

ZARZĄDZENIE Nr 13/2016

WÓJTA GMINY PUSZCZA MARIAŃSKA

z dnia 5 sierpnia 2016 r.

w sprawie **wprowadzenia polityki bezpieczeństwa w Urzędzie Gminy Puszcza Mariańska**

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 z późn. zm.), § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024) oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2016 r. poz. 464) zarządza się, co następuje:

§ 1.

W Urzędzie Gminy Puszcza Mariańska wprowadza się :

- 1/ politykę bezpieczeństwa o treści , stanowiącej załącznik nr 1 do niniejszego zarządzenia,
- 2/ instrukcję zarządzania systemem informatycznym o treści , stanowiącej załącznik nr 2 do niniejszego zarządzenia.

§ 2.

Zobowiązuje się wszystkich pracowników Urzędu Gminy Puszcza Mariańska do zapoznania się z niniejszym zarządzeniem i załącznikami do zarządzenia oraz do przestrzegania zasad zawartych w tych dokumentach.

Oświadczenie o zapoznaniu się należy wpiąć do akt osobowych pracowników .

§ 3.

Traci moc zarządzenie Nr 53/05 Wójta Gminy Puszcza Mariańska z dnia 29 grudnia 2005 r. w sprawie polityki bezpieczeństwa systemu informatycznego i Zarządzenie Nr 54/05 Wójta Gminy Puszcza Mariańska z dnia 29 grudnia 2005 r. w sprawie wprowadzenia Instrukcji zarządzania systemami informatycznymi oraz kartotekami przetwarzanymi przez Urząd Gminy w Puszczy Mariańskiej.

§ 4.

Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 5.

Zarządzenie wchodzi w życie z dniem podjęcia.

Michał Staniak
M. Malarz

WÓJT
Michał Staniak

POLITYKA BEZPIECZEŃSTWA URZĘDU GMINY PUSZCZA MARIAŃSKA

Rozdział 1

Postanowienia ogólne, definicje i objaśnienia

§ 1.1. Polityka bezpieczeństwa Urzędu Gminy Puszcza Mariańska jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Wójta Gminy Puszcza Mariańska .

2. Podstawą do opracowania i wdrożenia dokumentu są:

- 1) Konstytucja Rzeczypospolitej Polskiej;
- 2) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 z późn. zm.);
- 3) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 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 z późn. zm.).

3. Polityka bezpieczeństwa informacji Urzędu Gminy Puszcza Mariańska zawiera m.in:

- 1) wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe, stanowiący załącznik nr 1 do niniejszej polityki bezpieczeństwa informacji;
- 2) wykaz zbiorów danych osobowych przetwarzanych elektronicznie lub w inny sposób, stanowiący załącznik nr 2 do niniejszej polityki bezpieczeństwa informacji;
- 3) opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi, stanowiący załącznik nr 3 do niniejszej polityki bezpieczeństwa .

4. Przetwarzanie danych osobowych w Urzędzie Gminy Puszcza Mariańska jest dopuszczalne wyłącznie pod warunkiem przestrzegania przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych oraz Zarządzenia Wójta Gminy Puszcza Mariańska Nr 13/2016 z dnia 5 sierpnia 2016 r. wprowadzającego do Urzędu Gminy Puszcza Mariańska dokumentację przetwarzania danych osobowych.

§ 2. Użyte w treści polityki bezpieczeństwa informacji określenia oznaczają:

- 1) ustawa – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
- 2) dane osobowe – zestaw informacji pozwalających na jednoznaczną identyfikację konkretnej osoby w konkretnym środowisku pracy;
- 3) zbiór danych osobowych – dane osobowe zgromadzone w usystematyzowany sposób, pozwalający na łatwe dotarcie do konkretnej informacji;
- 4) przetwarzanie danych – wszystkie czynności wykonywane na danych, w tym szczególnie gromadzenie, utrwalanie, modyfikacja, usuwanie, przechowywanie, przenoszenie i przekazywanie, niezależnie od formy, w jakiej wykonywane są te czynności;
- 5) administrator danych osobowych – Wójt Gminy Puszcza Mariańska, osoba funkcyjna odpowiedzialna za całokształt zagadnień związanych z przetwarzaniem danych osobowych w administrowanych przez nią zbiorach danych;

- 6) administrator bezpieczeństwa informacji – osoba funkcyjna wyznaczana przez administratora danych osobowych, odpowiedzialna za przestrzeganie zasad ochrony danych osobowych i nadzorująca bezpieczeństwo przetwarzania danych osobowych w Urzędzie Gminy Puszcza Mariańska tj. Sekretarz Gminy;
- 7) administrator systemu informatycznego – osoba funkcyjna wyznaczana przez administratora danych osobowych odpowiedzialna za przestrzeganie zasad ochrony danych osobowych w systemie informatycznym i nadzorująca przetwarzanie danych osobowych w systemie informatycznym tj. podmiot obsługujący firma INFO-NET p. Agnieszka Markowska - Świetlik;
- 9) system informatyczny – zespół środków technicznych (urządzenia komputerowe, drukujące, łączności, wraz z okablowaniem i oprogramowaniem), zespół zabezpieczeń środków technicznych, użytkownicy tych urządzeń i programów, a także sieć informatyczna i udostępniane przez nią zasoby;
- 10) osoby zatrudnione przy przetwarzaniu danych osobowych, wszystkie osoby, w tym użytkownicy systemu informatycznego, mające – z racji wykonywanych obowiązków – dostęp do danych osobowych;

§ 3.1. Administrator danych osobowych ma obowiązek stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczać dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych osobowych określa zakres przetwarzanych danych osobowych w wydawanych zarządzeniach, regulaminach lub w indywidualnych umowach z podmiotami zewnętrznymi, którym może zlecić przetwarzanie danych osobowych.

3. Administrator danych osobowych przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach w określonych celach i w określonym zakresie, jeżeli:

- 1) jest to konieczne do realizacji określonych prawem zadań;
- 2) jest to niezbędne do osiągnięcia uzasadnionych celów;
- 3) w innym celu i zakresie, jeśli osoba, której przetwarzane dane dotyczą, wyrazi na to pisemną zgodę.

4. W przypadkach szczególnych cel i zakres przetwarzanych danych mogą określać inne obowiązujące przepisy szczegółowe.

§ 4.1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby wpisane do ewidencji prowadzonej przez administratora bezpieczeństwa informacji, które otrzymały stosowne upoważnienie.

2. Osoby zatrudnione w Urzędzie Gminy Puszcza Mariańska przy przetwarzaniu danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.

3. Osoby zatrudnione w Urzędzie Gminy Puszcza Mariańska przy przetwarzaniu danych osobowych przy wykorzystaniu systemów informatycznych są zobowiązane do postępowania zgodnie z „Instrukcją zarządzania systemem informatycznym” służącą do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów polityki bezpieczeństwa .

§ 5. Osoby zatrudnione przy przetwarzaniu danych są zobowiązane powiadomić administratora bezpieczeństwa informacji o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych w każdym zbiorze danych lub systemie. Tryb postępowania określa „Procedura alarmowa” stanowiąca załącznik do Instrukcji zarządzania systemem informatycznym.

§ 6. W zbiorach danych administrowanych przez Wójta Gminy Puszcza Mariańska zabrania się przetwarzania danych ujawniających:

- 1) stan zdrowia;
- 2) pochodzenie rasowe lub etniczne;
- 3) poglądy polityczne;
- 4) przekonania religijne lub filozoficzne;

- 5) przynależność wyznaniową;
 - 6) przynależność partyjną lub związkową;
 - 7) kod genetyczny;
 - 8) nałogi;
 - 9) preferencje seksualne,
- chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą, wyraziła pisemną zgodę.

§ 7. Pracownik, który:

- 1) przetwarza w zbiorze danych dane osobowe:
 - a) do których przetwarzania nie jest upoważniony,
 - b) których przetwarzanie jest zabronione,
 - c) niezgodne z celem stworzenia zbioru danych;
 - 2) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
 - 3) nie zgłasza administratorowi bezpieczeństwa informacji zbiorów danych podlegających rejestracji;
 - 4) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;
 - 5) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw;
- podlega odpowiedzialności karnej zgodnie z ustawą oraz sankcjami określonymi w Kodeksie pracy.

Rozdział 2

Gromadzenie danych osobowych

§ 8. Dane osobowe przetwarzane w Urzędzie Gminy Puszcza Mariańska mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 9.1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

Rozdział 3

Obowiązek informacyjny

§ 10.1. Urzędnicy na stanowiskach pracy, w których są zbierane i przetwarzane dane osobowe na innej podstawie niż podstawa znajdująca się w przepisie prawa, są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają, o:

- 1) adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane;
- 2) celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
- 3) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.

2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 ustawy.

§ 11.1. Materiały dotyczące innej niż ustawowa działalności Urzędu Gminy Puszcza Mariańska mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.

2. Kandydaci do pracy w Urzędzie Gminy Puszcza Mariańska w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.

3. Dokumenty złożone w celu określonym w ust. 2 są przechowywane w komórce organizacyjnej, która przetwarza te dane i są włączane do akt osobowych nowego pracownika bądź zwracane, w przypadku gdy osoba nie została zatrudniona..

Rozdział 4

Udzielanie informacji o przetwarzaniu danych osobowych

§ 12.1. Osobom, których dane osobowe przetwarza się w zbiorze danych Urzędu Gminy Puszcza Mariańska przysługuje, zgodnie z ustawą, prawo kontroli ich danych osobowych, a w szczególności – prawo do uzyskania wyczerpujących informacji na temat tych danych.

2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, powinna otrzymać odpowiedź w formie pisemnej, w miarę możliwości niezwłocznie, jednak w terminie nie dłuższym niż 14 dni od daty wpływu wniosku do Urzędu Gminy Puszcza Mariańska.

§ 13. W przypadku gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział 5

Rejestracja zbiorów danych osobowych

§ 14. Komórki organizacyjne Urzędu Gminy Puszcza Mariańska, w których przetwarzane są dane osobowe, są zobowiązane do zgłoszenia administratorowi bezpieczeństwa informacji na temat:

- 1) planowanego założenia nowych zbiorów danych osobowych wymagających rejestracji;
- 2) wnoszonych zmian do zbiorów już zarejestrowanych;
- 3) zaprzestania prowadzenia zarejestrowanych zbiorów danych osobowych.

Rozdział 6

Ochrona przetwarzania danych osobowych

§ 15.1. Administrator danych osobowych Urzędu Gminy Puszcza Mariańska zobowiązany jest do wydawania, ewidencjonowania i przechowywania imiennych upoważnień do przetwarzania danych osobowych oraz cofniętych upoważnień. Upoważnienie może zostać wydane na czas określony lub do odwołania. Wzór formularza upoważnienia stanowi załącznik nr 4 do niniejszej polityki bezpieczeństwa.

2. Administrator bezpieczeństwa informacji zobowiązany jest do zbierania, ewidencjonowania i przechowywania:

- 1) oświadczeń pracowników przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych.
- 2) oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy.
- 3) porozumień zawartych z osobami zatrudnionymi przy przetwarzaniu danych osobowych w zakresie wykorzystania oddanego im do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej.

3. Brak ważnego upoważnienia, o którym mowa w ust. 2 pkt 1, oraz brak podpisanych oświadczeń lub porozumienia, o których mowa w ust. 2 pkt 2 i pkt 3, uniemożliwia powierzenie pracownikowi wykonywania zadań i obowiązków związanych z przetwarzaniem danych osobowych.

§ 16.1. Całkowity nadzór i kontrolę przetwarzania danych osobowych w Urzędzie Gminy Puszcza Mariańska realizuje i odpowiada za te działania administrator bezpieczeństwa informacji.

2. Administrator bezpieczeństwa informacji ma obowiązek ściśle współpracować z administratorem systemu informatycznego w zakresie przetwarzania danych osobowych w systemach informatycznych.

3. Administrator bezpieczeństwa informacji ma obowiązek zapewnić zapoznanie się osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych oraz przeszkolić je w tym zakresie.

§ 17.1. W celu realizacji powierzonych zadań administrator bezpieczeństwa informacji w Urzędzie Gminy Puszcza Mariańska ma prawo:

- 1) kontrolować komórki organizacyjne Urzędu Gminy Puszcza Mariańska w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
- 2) wydawać polecenia pracownikom komórek organizacyjnych Urzędu Gminy Puszcza Mariańska w zakresie bezpieczeństwa danych osobowych;
- 3) informować administratora danych osobowych Urzędu Gminy Puszcza Mariańska o przypadkach naruszenia bezpieczeństwa danych osobowych;
- 4) żądać od wszystkich pracowników Urzędu Gminy Puszcza Mariańska wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

Rozdział 7

Zasady udostępniania danych osobowych

§ 18. Administrator danych osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 19.1. Zbiory danych osobowych udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.

2. Wniosek o udostępnienie danych osobowych powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.

3. Wniosek o udostępnienie danych osobowych jest rozpatrywany przez pracownika komórki organizacyjnej do której został dekretowany lub – w przypadku jego nieobecności przez pracownika zastępującego.

4. Pracownik komórki organizacyjnej prowadzi ewidencję wniosków o udostępnienie danych osobowych na merytorycznym stanowisku pracy.

§ 20. Administrator danych osobowych może odmówić udostępnienia danych osobowych, jeżeli spowodowałyby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy bądź wniosek jest sprzeczny z przepisami prawa.

§ 21.1. Administrator danych osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.

2. Podmiot, o którym mowa w ust. 1, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiory przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.

3. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.

WÓJT
Michał Staniak

Instrukcji zarządzania systemem informatycznym w Urzędzie Gminy Puszcza Mariańska

Rozdział 1

Przepisy ogólne

§ 1. Ilekroć w niniejszym dokumencie jest mowa o:

- 1) Urzędzie – należy przez to rozumieć jednostkę Urząd Gminy Puszcza Mariańska;
- 2) Administratorze Danych – należy przez to rozumieć Wójta Gminy Puszcza Mariańska ;
- 3) Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć Sekretarza Gminy Puszcza Mariańska ;
- 4) Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego Urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony ;
- 5) Użytkownika systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu,
- 6) Sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych jego 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 .

Rozdział 2

Procedury nadawania i zmiany uprawnień do przetwarzania danych

§ 2.1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych ma obowiązek zapoznać się z:

- 1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ;
- 2) rozporządzeniem 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 ;
- 3) Polityką bezpieczeństwa stanowiącą załącznik nr 1 do zarządzenia Wójta Gminy Puszcza Mariańska;
- 4) niniejszą instrukcją.

2. Zapoznanie się z przepisami wymienionymi w ust. 1 pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik Nr 1 do instrukcji.

3. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) Administratora Danych lub sporządzonego przez siebie, określającego zakres uprawnień pracownika.

4. Wzór wniosku o przyznanie uprawnienia w zakresie dostępu do systemu informatycznego stanowi załącznik Nr 2 do instrukcji.

5. Karta ewidencyjna powinna odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

6. Wzór karty ewidencyjnej, powinien zawierać:

- 1) imię i nazwisko użytkownika systemów informatycznych;
- 2) rodzaj uprawnienia;
- 3) datę nadania uprawnienia;
- 4) datę odebrania uprawnienia;
- 5) przyczynę odebrania uprawnienia;
- 6) podpis Administratora Bezpieczeństwa Informacji.

7. Wzór karty ewidencyjnej uprawnień w zakresie dostępu i obsługi programów i aplikacji systemu informatycznego w Urzędzie związanych z przetwarzaniem danych osobowych stanowi załącznik Nr 3 do instrukcji.

8. 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. Ustanowione hasło, Administrator Systemu Informatycznego przekazuje użytkownikowi ustnie. Identyfikator użytkownika składa się z sześciu znaków, z których dwa pierwsze odpowiadają dwóm pierwszym literom imienia użytkownika, a cztery kolejne odpowiadają pierwszym literom jego nazwiska. W identyfikatorze pomija się polskie znaki diaktryczne.

9. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

10. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

11. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą, jako naruszenie podstawowych obowiązków pracowniczych.

12. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

13. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.

14. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.

15. Odebranie uprawnień pracownikowi następuje na pisemny wniosek Administratora Danych lub Administratora Bezpieczeństwa Informacji, z podaniem daty oraz przyczyny odebrania uprawnień. Odebranie uprawnień pracownikowi równoważne jest z usunięciem konta pocztowego z serwera pocztowego wraz z jego zawartością.

16. Komórki organizacyjne Urzędu zobowiązane są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej sytuacji pracownika, mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.

17. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

18. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

Rozdział 3

Zasady posługiwania się hasłami

§ 3.1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i hasła.

2. Hasło powinno być zmieniane przez użytkownika, co najmniej raz w miesiącu.

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:

1) minimalna długość hasła - 8 znaków;

2) zakazuje się stosować:

a) haseł, które użytkownik stosował uprzednio w okresie minionego roku,

b) swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),

c) swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,

d) imion (w szczególności imion osób z najbliższej rodziny),

e) 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.,

f) wyrazów słownikowych,

g) przewidywalnych sekwencji znaków z klawiatury np.: "QWERTY", "12345678", itp.,

h) identyfikatorem użytkownika;

3) należy stosować:

a) hasła zawierające kombinacje liter i cyfr,

b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp., o ile system informatyczny na to pozwala,

c) hasła, które można zapamiętać bez zapisywania,

d) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.

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.

12. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:

- 1) Administrator Bezpieczeństwa Informacji;
- 2) Administrator Danych;
- 3) Administrator Systemu Informatycznego.

Rozdział 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

§ 4.1. Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.

2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wymeldowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.

3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wymeldowania z systemu.

4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej.

5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

Rozdział 5

Procedury tworzenia zabezpieczeń

§ 5.1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego.

2. Kopie bezpieczeństwa wykonywane są codzienne po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.

3. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest w pierwszym dniu każdego miesiąca w postaci zapisu na zewnętrznych dyskach twardej.

4. Zewnętrzne dyski twarde przechowuje się w zamykanej szafie w serwerowni Urzędu.

Rozdział 6

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

§ 6.1. Elektroniczne nośniki informacji:

- 1) dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa – zapisane na zewnętrznych nośnikach danych czy dyskach twardej nie są wynoszone poza siedzibę Urzędu;
- 2) wymienne w pkt 1 nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa;

- 3) po zakończeniu pracy przez użytkowników systemu, 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, uszkodza się w sposób uniemożliwiający ich odczytanie;
- 5) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

2. Kopie zapasowe:

- 1) kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w zamykanej szafie w serwerowni Urzędu;
- 2) dostęp do danych opisanych w punkcie 1 ma Administrator Bezpieczeństwa Informacji Administrator Systemu Informatycznego oraz upoważnieni przez Administratora Danych pracownicy.

3. 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

§ 7.1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.

2. Każdy e-mail wpływający do systemu informatycznego Urzędu musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.

3. Definicje wzorców wirusów aktualizowane są kilka razy w czasie dnia.

4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.

5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. 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 cykliczne kontrole antywirusowe na wszystkich komputerach - minimum, co trzy miesiące.

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.

Rozdział 8

Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

§ 8.1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.

2. Udostępnienie danych osobowych, w jakiegokolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.

3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną ani pocztą elektroniczną.

4. Udostępnienie danych osobowych następuje po przedstawieniu wniosku wg wzoru określonego w załącznik Nr 4 do instrukcji.

5. Pracownicy prowadzą rejestry udostępnionych danych osobowych zawierające, co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję, dla której dane udostępniono.

6. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować, co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

Rozdział 9

Postępowanie w sytuacji naruszenia ochrony danych osobowych

§ 9. Postępowanie w sytuacji naruszenia ochrony danych osobowych określa Instrukcja pn. „Procedura alarmowa” regulująca postępowanie pracowników Urzędu zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych stanowiąca załącznik Nr 5 do instrukcji.

Rozdział 10

Procedury wykonywania przeglądów i konserwacji systemu

§ 10.1. Przeglądy i konserwacja urządzeń:

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

2. Przegląd programów i narzędzi programowych:

- 1) konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów;
- 2) Administrator Bezpieczeństwa Informacji zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zameldowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję;
- 3) wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na płytę CD-R/DVD-R.

3. Rejestracja działań konserwacyjnych, awarii oraz napraw:

- 1) Administrator Systemu Informatycznego prowadzi „Dziennik systemu informatycznego Urzędu Gminy Puszcza Mariańska”, wzór i zakres informacji rejestrowanych w dzienniku określa załącznik Nr 6 do instrukcji;
- 2) wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego lub osoby przez nich wyznaczone.

Rozdział 11

Połączenie do sieci Internet

§ 11. Połączenie lokalnej sieci komputerowej Urzędu z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych (firewall) oraz kompleksowego oprogramowania antywirusowego.

Rozdział 12

Postanowienia końcowe

§ 12. Na stanowisku pracy obowiązuje bezwzględny zakaz instalowania jakiegokolwiek oprogramowania. Pracownik chcąc zainstalować aplikację lub program musi zgłosić taką potrzebę Administratorowi Systemu Informatycznego, który wyrażając zgodę na powyższe, odnotuje ten fakt w prowadzonym przez siebie Dzienniku..

W Ó J T
Michał Staniak

Załącznik nr 1
do Instrukcji zarządzania
systemem informatycznym

OŚWIADCZENIA O ZAPOZNANIU SIĘ Z PRZEPISAMI DOT. DANYCH OSOBOWYCH

....., dnia,
(miejscowość) (data)

.....
(imię i nazwisko)

.....
(stanowisko)

OŚWIADCZENIE

Oświadczam, iż w związku z wykonywaniem obowiązków służbowych, przetwarzam oraz mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym zapoznałem(am) się z:

- 1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135);
- 2) rozporządzeniem 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);
- 3) „POLITYKĄ BEZPIECZEŃSTWA URZĘDU GMINY PUSZCZA MARIAŃSKA wprowadzoną zarządzeniem Nr 13/2016 Wójta Gminy Puszcza Mariańska z dnia 5 sierpnia 2016 r. ;
- 4) „INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W URZĘDZIE GMINY PUSZCZA MARIAŃSKA wprowadzoną zarządzeniem Nr 13/2016 Wójta Gminy Puszcza Mariańska z dnia 5 sierpnia 2016 r. ;

.....
(podpis pracownika)

WNIOSEK O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

<input type="checkbox"/> Nowy użytkownik	<input type="checkbox"/> Nadanie uprawnień w systemie Informatycznym/modyfikacja	<input type="checkbox"/> Odebranie uprawnień w systemie informatycznym
Imię i nazwisko użytkownika		Stanowisko
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:		
Data wystawienia	Podpis bezpośredniego przełożonego użytkownika systemu:	
	Podpis Kierownika	

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do

2. Wnioskodawca

.....

.....

(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych:

.....

* ew. cd. w załączniku nr

4. Wskazanie przeznaczenia dla udostępnionych danych:

.....

* ew. cd. w załączniku nr

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:

.....

6. Zakres żądanych informacji ze zbioru:

.....

* ew. cd. w załączniku nr

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych:

.....

* ew. cd. w załączniku nr

.....

(data, podpis i ew. pieczęć wnioskodawcy)

„PROCEDURA ALARMOWA”

INSTRUKCJA REGULUJĄCA POSTĘPOWANIE PRACOWNIKÓW URZĘDU GMINY PUSZCZA MARIAŃSKA ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH.

§ 1. Niniejsza instrukcja reguluje postępowanie pracowników Urzędu Gminy Puszcza Mariańska zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych.

§ 2. Celem niniejszej instrukcji jest określenie zadań pracowników zatrudnionych przy przetwarzaniu danych osobowych w zakresie:

- 1) ochrony danych osobowych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą oraz ochroną zasobów technicznych;
- 2) w przypadku stwierdzenia naruszenia ochrony danych osobowych lub zabezpieczeń systemu informatycznego.

§ 3. Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:

- 1) stanu urządzeń technicznych;
- 2) zawartości zbiorów danych osobowych;
- 3) sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej;
- 4) metod pracy (w tym obiegu dokumentów).

§ 4. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy bezzwłocznie:

- 1) powiadomić Administratora Bezpieczeństwa Informacji lub bezpośredniego przełożonego lub Administratora Danych;
- 2) zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych;
- 3) podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia - o ile czynności te nie spowodują przekroczenia uprawnień pracownika;
- 4) zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.

§ 5.1. Bezpośredni przełożony pracownika po otrzymaniu powiadomienia o naruszenia bezpieczeństwa danych osobowych jest zobowiązany niezwłocznie powiadomić Administratora

Bezpieczeństwa Informacji lub Wójta Gminy chyba, że zrobił to pracownik, który stwierdził naruszenie.

2. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych Administrator Bezpieczeństwa Informacji przejmuje nadzór nad pracą w systemie odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji /brak naruszenia/.

§ 6. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona podejmuje czynności wyjaśniające mające na celu ustalenie:

- 1) przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych;

- 2) osób winnych naruszenia bezpieczeństwa danych osobowych;
- 3) skutków naruszenia.

§ 7.1. Administrator Bezpieczeństwa Informacji zobowiązany jest do powiadomienia o zaistniałej sytuacji Wójta Gminy, który podejmuje decyzje w zakresie wykonania czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.

2. Administrator Bezpieczeństwa Informacji zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, zawierającego, co najmniej:

- 1) datę i miejsce wystąpienia naruszenia;
- 2) zakres ujawnionych danych;
- 3) przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy;
- 4) sposób rozwiązania problemu;
- 5) przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

3. Raport ten Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych.

**DZIENNIK SYSTEMU INFORMATYCZNEGO URZĘDU GMINY PUSZCZA
MARIAŃSKA**

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:

- 1) w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- 2) w przypadku konserwacji/przeglądu systemu – opis podjętych działań, wnioski.

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania	Wnioski	Podpis

Załącznik nr 1
do Polityki bezpieczeństwa

WYKAZ BUDYNKÓW I POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

LP.	DOKŁADNY ADRES	STANOWISKO UŻYTKUJĄCE POMIESZCZENIE	NR POKOJU LUB POMIESZCZENIA	RODZAJ ZASTOSOWANEGO ZABEZPIECZENIA POMIESZCZENIA	UWAGI
1.	PUSZCZA MARIAŃSKA Ul. S. Papieżńskiego 1 96-330 Puszcza Mariańska	Wójt Gminy	Pokój nr 6	Pokój zamykany na klucz, System alarmowy	
2.		Samodzielne stanowisko ds. administracyjnych; Pomoc administracyjna	Sekretariat Pokój nr 8	Pokój zamykany na klucz, System alarmowy	Zbiory danych osobowych
3.		Sekretarz Gminy	Pokój nr 7	Pokój zamykany na klucz, System alarmowy	Zbiór danych osobowych
4.		Skarbnik Gminy	Pokój nr 23	Pokój zamykany na klucz, System alarmowy	
5.		Samodzielne stanowisko ds. gospodarki nieruchomościami	Pokój nr 22	Pokój zamykany na klucz, System alarmowy	Zbiory danych osobowych
6.		Samodzielne stanowisko ds. in- westycji;	Pokój nr 21	Pokój zamykany na klucz, System alarmowy	Bez zbioru danych osobowych;

		Samodzielne stanowisko ds. dróg i budynków				Zbiory danych osobowych
7.		Samodzielne stanowisko ds. obywatelskich	Pokój nr 20	Pokój zamykany na klucz, System alarmowy, Krata w oknie		Zbiory danych osobowych
8.		Referat Finansowy	Pokój nr 19	Pokój zamykany na klucz, System alarmowy, Krata w oknie		Zbiory danych osobowych
9.		Referat Finansowy	Pokój nr 18	Pokój zamykany na klucz, System alarmowy		Zbiory danych osobowych
10.		Referat Finansowy	Pokój nr 17 Kasa	Pokój zamykany na klucz, System alarmowy, Krata w oknie		
11.		Samodzielne stanowisko ds. obsługi rady gminy i działalności gospodarczej	Pokój nr 14	Pokój zamykany na klucz, System alarmowy		Zbiory danych osobowych
12.		Samodzielne stanowisko ds. gospodarki komunalnej, zarządzania kryzysowego i obrony cywilnej; Samodzielne stanowisko ds. obsługi finansowej gospodarki odpadami	Pokój nr 13	Pokój zamykany na klucz, System alarmowy		Zbiory danych osobowych Bez zbioru danych osobowych

13.	Referat Finansowy	Pokój nr 12	Pokój zamykany na klucz, System alarmowy, Krata w oknie	Zbiór danych osobowych
14.	Referat Finansowy	Pokój nr 11	Pokój zamykany na klucz, System alarmowy Krata w oknie	Zbiory danych osobowych
15.	Samodzielne stanowisko ds. zagospodarowania przestrzennego Samodzielne stanowisko ds. ochrony środowiska	Pokój nr 9	Pokój zamykany na klucz, System alarmowy	Zbiory danych osobowych Zbiory danych osobowych
16.	Samodzielne stanowisko ds. gospodarki komunalnej Samodzielne stanowisko ds. gospodarki lokalowej	Pokój nr 10	Pokój zamykany na klucz, System alarmowy	Zbiory danych osobowych Zbiory danych osobowych
17.	Kierownik Urzędu Stanu Cywilnego Z-ca Kierownika USC	Pokój nr 5 (4)	Pokój zamykany na klucz, System alarmowy, Krata w oknie	Zbiory danych osobowych Zbiory danych osobowych
18.	Kierownik USC, Z-ca Kierownika USC	Pokój nr 1	Pokój zamykany na klucz, System alarmowy, Pomieszczenie bez okna	Archiwum dowodów osobistych i usc

19.		Samodzielne stanowisko ds. obsługi rady gminy i działalności gospodarczej	Piwnica budynku Urzędu Gminy, dwa pomieszczenia	Pomieszczenia zamknięte na klucz	
20.	Puszcza Mariańska Pl. Tadeusza Kościuszki 2, 96-330 Puszcza Mariańska	Sekretarz Gminy	Pomieszczenia obsługujące Gminną Komisję Rozwiązywania Problemów Alkoholowych	Pomieszczenie zamknięte na klucz	

WYKAZ ZBIORÓW DANYCH OSOBOWYCH W URZĘDZIE GMINY PUSZCZA MARIAŃSKA

Lp	Nazwa zbioru danych	Stanowisko pracy prowadzące zbiór	Programy zastosowane do przetwarzania danych	Uwagi
1.	Wnioski o zezwolenie na utrzymanie psa rasy agresywnej	Samodzielne stanowisko ds. ochrony środowiska	Office (Word)	Zbiór rejestrowany w 2016 r. przez ABI
2.	Dane strażaków OSP	Samodzielne stanowisko ds. ochrony środowiska	Office (Word)	Zbiór rejestrowany w 2016 r. przez ABI
3.	Wnioski o wycinkę drzew	Samodzielne stanowisko ds. ochrony środowiska	Office (Word), e-Doś	Zbiór rejestrowany w 2004 r. przez GIODO
4.	Wnioski o wydanie decyzji środowiskowych	Samodzielne stanowisko ds. ochrony środowiska	Office (Word), e-Doś	Zbiór rejestrowany w 2016 r. przez ABI
5.	Rejestr wyrobów zawierających azbest	Samodzielne stanowisko ds. ochrony środowiska	Office (Word), „Baza Azbestowa” w sieci Internet	Zbiór rejestrowany w 2016 r. przez ABI
6.	Radni Gminy Puszcza Mariańska	Samodzielne stanowisko ds. obsługi Rady Gminy i działalności gospodarczej	Biuletyn Informacji Publicznej w sieci Internet	Aktualizacja zbioru „Oświadczenia o stanie majątkowym radnych” zgłoszonego do GIODO w 2000 r.
7.	Zezwolenia na sprzedaż napojów alkoholowych	Samodzielne stanowisko ds. obsługi Rady Gminy i działalności gospodarczej	Office (Word), systemy dziedzinowe: „system zezwoleń na sprzedaż napojów alkoholowych”	Zbiór rejestrowany przez ABI w 2016 r.
8.	Rejestr wniosków o wpis do CE-IDG	Samodzielne stanowisko ds. obsługi Rady Gminy i działalności gospodarczej	Portal CEIDG w sieci Internet administrowany przez Ministra Rozwoju	Zbiór rejestrowany w 2016 r. przez ABI
9.	Zbiór podatników osoby fizyczne i prawne	Referat Finansowy /pok. Nr 18/	Program Radix's - POGRUN , Office	Aktualizacja zbioru „Zbiór podatników” zgłoszonego do GIODO w 2000 r. /zgłosz. 2000 r./

10.	Ewidencja płatników i dłużników	Referat Finansowy /pok. Nr 19/	Program Radix's WIP, Office	Aktualizacja zbioru „Zbiór płatników i dłuż- ników” zgłoszonego do GIODO w 2000 r.
11.	Użytkownicy sieci kanalizacyjnej	Samodzielne stanowisko ds. go- spodarki komunalnej	Program Radix's – REJ+ Office	Aktualizacja zbioru „Zbiór użytkowników sieci kanalizacyjnej” zgłoszonego do GIODO w 2000 r.
12.	Użytkownicy sieci wodociągowej	Samodzielne stanowisko ds. go- spodarki komunalnej	Program Radix's – REJ+ Office	Aktualizacja zbioru „Zbiór użytkowników sieci wodociągowej” zgłoszonego do GIODO w 2000 r.
13.	Dowody osobiste	USC /pok. Nr 5/	System Rejestrów Państwowych ŹRÓ- DŁO w sieci internet (RDO) , administro- wany przez Ministra Administracji i Cy- fryzacji, Office	Aktualizacja „Zbiór osób, którym wydano do- wody osobiste” zgłoszo- nego do GIODO 2000 r.
14.	Urząd Stanu Cywilnego – księgi stanu cywilnego i akta zbiorowe	USC /pok. Nr 5/	System Rejestrów Państwowych ŹRÓ- DŁO w sieci internet (BUSC) , admini- strowany przez Ministra Administracji i Cyfryzacji, Office	Aktualizacja zbioru „Urząd Stanu cywilnego w Puszczy Mariańskiej” zgłoszonego do GIODO w 2000 r.
15.	Rejestr mieszkańców	Z-ca Kierownika USC /pok. Nr 5/	System Rejestrów Państwowych ŹRÓ- DŁO w sieci internet (PESEL) , admini- strowany przez Ministra Administracji i Cyfryzacji, Program Radix's – ELUD, Office	Aktualizacja zbioru „Ewidencja ludności” zgłoszonego do GIODO w 2000 r.
16.	Rejestr zamieszkania cudzoziem- ców	Z-ca Kierownika USC /pok. Nr 5/	Program Radix's – ELUD , Office	Zbiór rejestrowany w 2016 r. przez ABI
17.	Kwalifikacja wojskowa	Z-ca Kierownika USC	System Rejestrów Państwowych ŹRÓ- DŁO w sieci internet (PESEL) , admini- strowany przez Ministra Administracji i	Aktualizacja zbioru „Ewidencja przedpoboro- wych i poborowych”

				Cyfrizacji, Program Radix's – ELUD, Office	zgłoszonego w GIODO w 2000 r.
18.	Wnioski o wydanie warunków zabudowy	Samodzielne stanowisko ds. zagospodarowania przestrzennego	Office	Office,	Aktualizacja zbioru „Decyzje ustalające sposób zagospodarowania terenu i podziału nieruchomości” zgłoszonego do GIODO w 2000
19.	Wnioski o ustalenie lokalizacji inwestycji celu publicznego	Samodzielne stanowisko ds. zagospodarowania przestrzennego	Office	Office	Zbiór rejestrowany w 2016 r. przez ABI
20.	Wnioski o opinie wstępnych projektów podziałów	Samodzielne stanowisko ds. zagospodarowania przestrzennego	Office	Office	Zbiór rejestrowany w 2016 r. przez ABI
21.	Wnioski o wydanie wypisów i wrysów z MPZP oraz Studium	Samodzielne stanowisko ds. zagospodarowania przestrzennego	Office	Office	Zbiór rejestrowany w 2016 r. przez ABI
22.	Wnioski o zmianę MPZP	Samodzielne stanowisko ds. zagospodarowania przestrzennego	Office	Office	Zbiór rejestrowany w 2016 r. przez ABI
23.	Wnioski o zmianę studium uwarunkowań i kierunków zagospodarowania przestrzennego	Samodzielne stanowisko ds. zagospodarowania przestrzennego	Office	Office	Zbiór rejestrowany w 2016 r. przez ABI
24.	Zbiór wnioskodawców korzystających z dróg w sposób szczególny	Samodzielne stanowisko ds. dróg i budynków	Systemy dziedzinowe: „system ewidencji zezwoleń na lokalizację w pasie drogowym”, Office	Office	Zbiór rejestrowany w 2016 r. przez ABI
25.	Dowóz uczniów niepełnosprawnych do szkół	Samodzielne stanowisko ds. obywatelskich	Office	Office	Zbiór do zarejestrowania u GIODO
26.	System Informacji Oświatowej	Samodzielne stanowisko ds. obywatelskich	Platforma SIO w sieci Internet administrowana przez , Office	Office	Zbiór rejestrowany przez ABI w 2016 r.
27.	Awans zawodowy na stopień nauczyciela mianowanego	Samodzielne stanowisko ds. obywatelskich	Office	Office	Zbiór rejestrowany przez ABI w 2016 r.
28.	Stypendia za wyniki w nauce i osiągnięcia sportowe	Samodzielne stanowisko ds. obywatelskich	Office	Office	Zbiór rejestrowany przez ABI w 2016 r.

29.	Zbiór danych osobowych świadczących świadczenia z funduszu alimentacyjnego i dłużników alimentacyjnych w Urzędzie Gminy Puszcza Mariańska	Samodzielne stanowisko ds. obywatelskich	Program Sygnity – program do obsługi Funduszu Alimentacyjnego wraz z modulem Windykacje, Office	Zbiór do zarejestrowania u GIODO
30.	„Zbiór osób otrzymujących podatki mieszkaniowe”	Samodzielne stanowisko ds. gospodarki lokalowej	Office	Aktualizacja zbioru „Zbiór osób otrzymujących podatki mieszkaniowe” zgłoszonego do GIODO w 2000 r.
31.	Najem lokali mieszkaniowych	Samodzielne stanowisko ds. lokalowej	Office	Aktualizacja zbioru „Zbiór najemców lokali mieszkalnych” Zgłoszonego do GIODO w 2000 r.
32.	Rejestr skarg i wniosków	Samodzielne stanowisko ds. administracyjnych	Office	Aktualizacja zbioru „Ewidencja skarg i wniosków” zgłoszonego do GIODO w 2000 r.
33.	Rejestr przyjęć interesantów	Samodzielne stanowisko ds. administracyjnych		Zbiór rejestrowany przez ABI w 2016 r.
34.	Dziennik korespondencji	Samodzielne stanowisko ds. administracyjnych	Systemy dziedzinowe – system Elektronicznego Zarządzania Dokumentacją (EZD)	Zbiór rejestrowany przez ABI w 2016 r.
35.	Ewidencja płatników i dłużników opłaty za gospodarowanie odpadami komunalnymi	Samodzielne stanowisko ds. obsługi finansowej gospodarki odpadami	Programy Radix’s – WIP, Office	Zbiór rejestrowany przez ABI w 2016
36.	Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi	Samodzielne stanowisko ds. gospodarki komunalnej, zarządzania kryzysowego i obrony cywilnej	Programy Radix’s - GOK, Office	Zbiór rejestrowany przez ABI w 2016 r.

37.	Świadczenia osobiste i rzeczowe	Samodzielne stanowisko ds. gospodarki komunalnej, zarządzania kryzysowego i obrony cywilnej	Office	Zbiór rejestrowany przez ABI w 2016 r.
38.	Czystość i porządek na terenie gminy – obowiązek mieszkańców	Samodzielne stanowisko ds. gospodarki komunalnej, zarządzania kryzysowego i obrony cywilnej	Office	Zbiór rejestrowany przez ABI w 2016 r.
39.	Rozgraniczenia nieruchomości	Samodzielne stanowisko ds. gospodarki nieruchomościami	Office	Zbiór rejestrowany przez ABI w 2016 r.
40.	Podziały nieruchomości	Samodzielne stanowisko ds. gospodarki nieruchomościami	Office	Aktualizacja zbioru „Ewidencja decyzji o podziałach” zgłoszonego do GIODO w 2000 r.
41.	Szkody w rolnictwie	Samodzielne stanowisko ds. gospodarki nieruchomościami	Office	Zbiór rejestrowany przez ABI w 2016 r.
42.	Zwrot podatku akcyzowego dla rolników	Samodzielne stanowisko ds. gospodarki nieruchomościami	Program ZWROTY, Office	Zbiór rejestrowany przez ABI w 2016 r.
43.	pomoc materialna dla uczniów	Referat Finansowy /pok. Nr 11/	Office	Aktualizacja zbioru zgłoszonego do GIODO w 2005 r.; aktualizacja zbioru u GIODO
44.	Osoby objęte postępowaniem GKRPA	Gminna Komisja Rozwiązywania Problemów Alkoholowych, Sekretarz Gminy	Office	Aktualizacja zbioru „Przeciwdziałanie alkoholizmowi”, zgłoszonego do GIODO w 2000 r. aktualizacja zbioru u GIODO
45.	Przeciwdziałanie alkoholizmowi	Gminna Komisja Rozwiązywania Problemów Alkoholowych, Sekretarz Gminy	Office	Zbiór rejestrowany przez ABI w 2016 r.
46.	Decyzje nakazujące właścicielowi nieruchomości usunięcie odpadów	Samodzielne stanowisko ds. gospodarki komunalnej, zarządzania kryzysowego i obrony cywilnej	Office	Zbiór rejestrowany przez ABI w 2016 r.

**OPIS STRUKTURY ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMACH
INFORMATYCZNYCH I SPOSÓB PRZEPLYWU DANYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI**

Lp	Nazwa zbioru danych	Struktura zbiorów	Przeływ danych	Uwagi
1.	Wnioski o zezwolenie na utrzymanie psa rasy agresywnej	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu 	Wydruk z Office (Word)	
2.	Dane strażaków OSP	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania/pobytu - numer telefonu - numer pesel - Numer Identyfikacji Podatkowej - miejsce pracy - zawód - wykształcenie - seria i numer dowodu osobistego 	Wydruk z Office (Word)	
3.	Wnioski o wycinkę drzew	<ul style="list-style-type: none"> - nazwiska i imiona - data urodzenia - miejsce urodzenia - adres zamieszkania/pobytu - numer telefonu - seria i numer dowodu osobistego - numer ewidencyjny nieruchomości 	Zamieszczenie części danych w sieci Internet, wydruk z Office (word)	

4.	Wnioski o wydanie decyzji środowiskowych	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości - numer pesel - Numer Identyfikacji Podatkowej 	Zamieszczenie części danych w sieci Internet, wydruk z Office (word)	
5.	Rejestr wyrobów zawierających azbest	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości 	Zamieszczenie części danych w sieci Internet, wydruk z Office (word)	
6.	Radni Gminy Puszcza Mariańska	<ul style="list-style-type: none"> - nazwiska i imiona - data urodzenia - miejsce urodzenia - adres zamieszkania lub pobytu - miejsce pracy - zawód - wykształcenie - numer telefonu - dane o nieruchomości - zasoby pieniężne - tytuły prawne do nieruchomości - składniki mienia ruchomego - udziały w spółkach - zobowiązania pieniężne - adresy nieruchomości 	Wprowadzenie na stronę BIP w sieci Internet, Wydruk z Office	
7.	Zezwolenia na sprzedaż napojów alkoholowych	<ul style="list-style-type: none"> - nazwiska i imiona - Numer Identyfikacji Podatkowej - numer telefonu - oznaczenie przedsiębiorcy - siedziba adres) przedsiębiorcy - dane pełnomocników 	Wydruk z Office	

8.	Rejestr wniosków o wpis do CE-IDG	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - Numer Identyfikacji Podatkowej - - seria i numer dowodu osobistego - numer telefonu - numer rachunku bankowego - dane pełnomocnika 	Dane wprowadzane na Portal CEIDG w sieci Internet , wydruk z Internetu	
9.	Zbiór podatników osoby fizyczne i prawne	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - seria i numer dowodu osobistego - numer telefonu 	Wydruk z Program Radix's - POGRUN , Office	
10.	Ewidencja płatników i dłużników	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców - data urodzenia - adres zamieszkania lub pobytu - numer pesel - Numer Identyfikacji Podatkowej 	Wydruk z systemu WIP, z Office	
11.	Użytkownicy sieci kanalizacyjnej	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania lub pobytu - numer pesel - seria i numer dowodu osobistego - numer telefonu - numer ewidencyjny nieruchomości 	Wprowadzenie i wydruk z Program Radix's – REJ+ , z Office	

12.	Użytkownicy sieci wodociągowej	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania lub pobytu - numer pesel - seria i numer dowodu osobistego - numer telefonu - numer ewidencyjny nieruchomości 	Wprowadzenie i wydruk z Program Radix's – REJ+ , z Office	
13.	Dowody osobiste	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - seria i numer dowodu osobistego - numer telefonu - nazwisko rodowe matki - płeć - obywatelstwo 	Wprowadzenie do Systemu Rejestrów Państwowych ŹRÓDŁO w sieci internet (RDO) , wydruk z OFFice	
14.	Urząd Stanu Cywilnego – księgi stanu cywilnego i akta zbiorowe	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - seria i numer dowodu osobistego - wykształcenie - nazwisko rodowe rodziców - stan cywilny - numer telefonu 	Wydruk z Systemu Rejestrów Państwowych ŹRÓDŁO w sieci internet (BUSC), Office	

15.	Rejestr mieszkańców	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - seria i numer dowodu osobistego - nazwisko rodowe - nazwisko rodowe rodziców - kraj urodzenia - stan cywilny - akt urodzenia i USC jego sporządzenia - płeć - obywatelstwo - imię i nazwisko rodowe małżonka - pesel małżonka - adres i data zameldowania na pobyt stały 	<p>Wydruk z Systemu Rejestrów Państwowych ŹRÓDŁO w sieci internet, Programu Radix's, Office</p>	
16.	Rejestr zamieszkania cudzoziemców	<ul style="list-style-type: none"> - nazwiska i imiona - data urodzenia, - miejsce urodzenia - numer pesel - kraj urodzenia 	<p>Wydruk z Systemu Rejestrów Państwowych ŹRÓDŁO w sieci internet (PESEL), z Office</p>	
17.	Kwalifikacja wojskowa	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - numer pesel - seria i numer dowodu osobistego - nazwisko rodowe - nazwisko rodowe rodziców - płeć - adres i data zameldowania na pobyt stały 	<p>Wydruk z Systemu Rejestrów Państwowych ŹRÓDŁO w sieci internet (PESEL)</p>	

18.	Wnioski o wydanie warunków zabudowy	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	Wydruk z Office (word)	
19.	Wnioski o ustalenie lokalizacji inwestycji celu publicznego	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	Wydruk z Office (word)	
20.	Wnioski o opinie wstępnych projektów podziałów	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	Wydruk z Office (word)	
21.	Wnioski o wydanie wypisów i wrysów z MPZP oraz Studium	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	Wydruk z Office (word)	
22.	Wnioski o zmianę MPZP	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	Wydruk z Office (word)	
23.	Wnioski o zmianę studium uwarunkowań i kierunków zagospodarowania przestrzennego	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	Wydruk z Office (word)	
24.	Zbiór wnioskodawców korzystających z dróg w sposób szczególny	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	- nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości	Wydruk z Office (word)	

25.	Dowóz uczniów niepełnosprawnych do szkół	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - wykształcenie - numer rachunku bankowego - rodzaj niepełnosprawności - numer i seria prawa jazdy, <p>Ważliwe:</p> <ul style="list-style-type: none"> - stan zdrowia 	<p>Wydruk z Office</p>	
26.	System Informacji Oświatowej	<ul style="list-style-type: none"> - nazwiska i imiona - data urodzenia, - numer pesel - miejsce pracy - zawód - wykształcenie 	<p>Zamieszczenie danych na portalu SIO w sieci</p>	
27.	Awans zawodowy na stopień nauczyciela mianowanego	<ul style="list-style-type: none"> - nazwiska i imiona - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - seria i numer dowodu osobistego - miejsce pracy - zawód - wykształcenie - numer telefonu 	<p>Wydruk z Office</p>	
28.	Stypendia za wyniki w nauce i osiągnięcia sportowe	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - adres zamieszkania lub pobytu - wykształcenie - numer telefonu - numer rachunku bankowego 	<p>Wydruk z Office</p>	

29.	<p>Zbiór danych osobowych świadczonych przez Fundację z Funduszu Alimentacyjnego i dłużników alimentacyjnych w Urzędzie Gminy Puszcza Mariańska</p>	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - Numer Identyfikacji Podatkowej - miejsce pracy - zawód - wykształcenie - seria i numer dowodu osobistego - numer telefonu - dochody członków rodziny - dane członków rodziny - nazwisko rodowe - stan zadłużenia dłużnika alimentacyjnego - informacje o sytuacji rodzinnej dłużnika alimentacyjnego, - informacje o sytuacji dochodowej i zawodowej dłużnika alimentacyjnego - seria i numer prawa jazdy - zawód wyuczony - zawód wykonywany - nazwisko rodowe matki <p>Ważliwe:</p> <ul style="list-style-type: none"> - stan zdrowia - nałogi - skazania - orzeczenia o ukaraniu - inne orzeczenia wydawane w postępowaniu sądowym lub administracyjnym 	<p>Wprowadzane i drukowane z systemu Sygnity, wydruk z Office</p>	
30.	<p>„Zbiór osób otrzymujących dotki mieszkaniowe”</p>	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - seria i numer dowodu osobistego 	<p>Wydruk z Office</p>	
31.	<p>Najem lokali mieszkaniowych</p>	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania lub pobytu - seria i numer dowodu osobistego 	<p>Wydruk z Office</p>	

32.	Rejestr skarg i wniosków	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania lub pobytu 	Wydruk z Office	
33.	Rejestr przyjęć interesantów	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania lub pobytu - numer telefonu 		
34.	Dziennik korespondencji	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania lub pobytu - numer ewidencyjny pesel - Numer Identyfikacji Podatkowej - numer telefonu 	Wydruk z systemu Elektronicznego Zarządzania Dokumentacją (EZD)	
35.	Ewidencja płatników i dłużników opłaty za gospodarowanie odpadami komunalnymi	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - adres zamieszkania lub pobytu - numer pesel - Numer Identyfikacji Podatkowej 	Wydruk z Programy Radix's – WIP, Office	
36.	Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - adres zamieszkania lub pobytu - numer pesel - numer telefonu 	Wprowadzenie danych do programu GOK i wydruk, wydruk z Office	
37.	Świadczenia osobiste i rzeczowe	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania lub pobytu 	Wydruk z Office	
38.	Czystość i porządek na terenie gminy – obowiązek mieszkańców	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania lub pobytu - numer telefonu 	Wydruk z Office	
39.	Rozgraniczenia nieruchomości	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości 	Wydruk z Office	
40.	Podziały nieruchomości	<ul style="list-style-type: none"> - nazwiska i imiona 	Wydruk z Office	

41.	Szkody w rolnictwie	<ul style="list-style-type: none"> - imiona rodziców - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny nieruchomości 	Wydruk z Office		
42.	Zwrot podatku akcyzowego dla rolników	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania/pobytu - numer telefonu - numer ewidencyjny pesel 	Wydruk z programu obsługującego		
43.	Pomoc materialna dla uczniów	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - miejsce pracy - zawód - seria i numer dowodu osobistego - numer telefonu - dochody członków rodziny - uzyskana pomoc społeczna członków rodziny - dane członków rodziny - informacje o sytuacji rodzinnej - informacje o sytuacji dochodowej <p>Ważliwe:</p> <ul style="list-style-type: none"> - stan zdrowia - nałogi 	Wydruk z Office	Większość danych osobowych bez konieczności wydruku	
44.	Osoby objęte postępowaniem GKRPA	<ul style="list-style-type: none"> - nazwiska i imiona - imiona rodziców, - data urodzenia, 	Wydruk z Office	Elementy zbioru przekazywane do Sądu Rejonowego,	

		<ul style="list-style-type: none"> - miejsce urodzenia - adres zamieszkania lub pobytu - numer pesel - miejsce pracy - zawód - seria i numer dowodu osobistego - numer telefonu - dane członków rodziny - nazwisko rodowe - informacje o sytuacji rodzinnej - informacje o sytuacji dochodowej rodziny <p>Wrażliwe:</p> <ul style="list-style-type: none"> - stan zdrowia - nałogi - skazania - orzeczenia o ukaraniu - inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym 		Wydział Rodzinny i Nieletnich
45.	Przeciwdziałanie alkoholizmowi	<ul style="list-style-type: none"> - nazwiska i imiona - data urodzenia - adres zamieszkania lub pobytu - numer ewidencyjny pesel - numer telefonu 	Wydruk z Office	
46.	czystość i porządek na terenie gminy – obowiązek mieszkańców	<ul style="list-style-type: none"> - nazwiska i imiona - adres zamieszkania lub pobytu - numer telefonu 	Wydruk z Office	

Załącznik nr 4

do Polityki bezpieczeństwa

Upoważnienie do przetwarzania danych osobowych

.....
/nazwisko i imię pracownika/

Puszcza Mariańska dn.

.....
/stanowisko/

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (.....)

upoważniam Pana/Panią

do dostępu i przetwarzania danych osobowych zawartych w kartotekach oraz w systemie informatycznym, do obsługi systemu informatycznego i urządzeń wchodzących w jego skład w

Urzędzie Gminy Puszcza Mariańska

.....
/wskazać stanowisko pracy, pokój/

na powierzonym stanowisku pracy i w związku z czynnościami wykonywanymi na tym stanowisku pracy .

Identyfikator

Upoważnienie obejmuje prawo wglądu, modyfikacji i usuwania danych osobowych w zasobach przetwarzanych na w/w stanowisku pracy, w tym w zbiorze danych osobowych:

.....
.....
Upoważniony pracownik zobowiązuje się do przestrzegania zasad ustalonych w Urzędzie Gminy Puszcza Mariańska , w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa” oraz respektowania zapisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych . Upoważnionemu obowiązuje obowiązek zachowania w tajemnicy danych osobowych przetwarzanych w Urzędzie oraz sposobów zabezpieczeń.

/odpis niniejszego upoważnienia znajduje się w aktach osobowych pracownika/.

Przyjmuję:

.....
/data i podpis pracownika/

.....
/podpis Wójta Gminy bądź ABI/