**ZARZĄDZENIE NR 223./2013**
**BURMISTRZA ORZYSZA**

z dnia 31 października 2013 r.

**w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych**

Na podstawie art. 33, ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j Dz. U. z 2013 r., poz. 594 z późn. zm.), art. 26 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (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. Nr 100, poz. 1024), zarządzam, co następuje:

**§ 1.**

Ustalam:

1) Politykę bezpieczeństwa Urzędu Miejskiego w Orzyszu - stanowiącą załącznik nr 1,

2) Instrukcję zarządzania systemem informatycznym Urzędu Miejskiego w Orzyszu stanowiącą załącznik nr 2.

**§ 2.**

Wykonanie Zarządzenia powierza się Sekretarzowi Gminy Orzysz.

**§ 3.**

Traci moc zarządzenie Nr 5/99 Burmistrza Miasta i Gminy w Orzyszu z dnia 5 października 1999 r. wprowadzające instrukcję w sprawie zabezpieczenia dokumentów zawierających dane osobowe, instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz instrukcję postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

**§ 4.**

Zarządzenie wchodzi w życie z dniem 1 listopada 2013 r.

BURMISTRZ
mgr Tomasz Jakub Sulima

Załącznik Nr 1 do Zarządzenia Nr 223/2013
Burmistrza Orzysza
z dnia 31.10.... 2013 r.

**Polityka bezpieczeństwa Urzędu Miejskiego w Orzyszu**

## Rozdział 1.
## Postanowienia ogólne

### § 1.

1. Polityka bezpieczeństwa dotycząca przetwarzania danych osobowych w Urzędzie Miejskim w Orzyszu, 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 w innych zbiorach ewidencyjnych,
   b) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
2. Urząd Miejski w Orzyszu, zwany dalej „Urzędem", realizując Politykę dokłada szczególnej staranności w celu zabezpieczenia bezpieczeństwa danych osobowych poprzez zapewnienie ich poufności, integralności i dostępności, w tym w szczególności 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. Urząd realizując Politykę dąży do systematycznego optymalnego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Polityka obowiązuje wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w Urzędzie.
5. Polityka została opracowana na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwaną dalej „ustawą o ochronie danych osobowych", oraz 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)
6. Polityka bezpieczeństwa podlega okresowej aktualizacji, która jest realizowana przez Administratora Bezpieczeństwa Informacji.

### § 2.

Ilekroć w Polityce jest mowa o:

1) Administratorze Danych Osobowych – zwanym dalej Administratorem należy przez to rozumieć Gminę Orzysz reprezentowaną przez Burmistrza Orzysza,

2) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ze zmianami,

3) danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,

4) danych osobowych wrażliwych – rozumie się przez to dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazania, orzeczeń o ukaraniu i mandatach karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym,

5) 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,

6) Urzędzie – rozumie się przez to Urząd Miejski w Orzyszu,

7) Instrukcji – rozumie się przez to Instrukcję zarządzania systemem informatycznym, która obowiązuje w Urzędzie Miejskim w Orzyszu,

8) Administratorze Bezpieczeństwa Informacji, zwanym dalej ABI - należy przez to rozumieć osobę wyznaczoną przez Administratora Danych Osobowych i odpowiedzialną za nadzorowanie przestrzegania zasad ochrony przetwarzanych danych osobowych w Urzędzie, w tym w szczególności związanych z przeciwdziałaniem dostępowi do danych osobowych osób nieupoważnionych, zabraniu przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem oraz przetwarzaniem danych z naruszeniem ustawy o ochronie danych osobowych,

9) Merytorycznym Administratorze Informacji, zwanym dalej MAI – należy przez to rozumieć kierującego referatem urzędu właściwą dla danego zakresu danych osobowych, który jest odpowiedzialny merytorycznie za przetwarzanie danych w określonym zakresie i jest właścicielem zbioru,

10) Administratorze Systemów Informatycznych, zwanym dalej ASI - należy przez to rozumieć pracownika oraz inną osobę lub osoby wyznaczone przez Administratora Systemu, których celem działania jest nadzorowanie, kontrolowanie zasad bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych,

11) użytkowniku - należy przez to rozumieć pracownika Urzędu (osoba wykonująca pracę na podstawie umowy o pracę, powołania, wyboru lub umowy cywilnoprawnej), który posiada upoważnienie wydane przez Administratora Danych Osobowych i dopuszczony jest (w zakresie w nim wskazanym) do przetwarzania danych osobowych w danej jednostce organizacyjnej urzędu,

12) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący 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) osobie trzeciej – należy przez to rozumieć każdą osobę nieupoważnioną i przez to nieuprawnioną do dostępu do danych osobowych będących w posiadaniu Administratora. Osobą trzecią jest również

osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych podejmująca czynności w zakresie przekraczającym ramy tego upoważnienia,

15) systemie informatycznym, zwanym dalej systemem – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

16) zabezpieczeniu systemu informatycznego – należy przez to rozumieć wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią,

17) 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,

18) usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

19) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom (osobom),

20) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

21) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu (użytkownika) mogą być przypisane w sposób jednoznaczny temu podmiotowi (użytkownikowi),

21) uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (użytkownika),

23) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) przedstawiciela podmiotu przetwarzającego dane osobowe mającego siedzibę lub miejsce zamieszkania w państwie trzecim,

d) podmiotu, któremu powierzono przetwarzanie danych osobowych w drodze umowy,

e) 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 jest dopuszczalne tylko wtedy, gdy:

a) osoba, której dane dotyczą, wyrazi zgodę, chyba że chodzi o usunięcie dotyczących jej danych,

b) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu 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 i wolności 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 osobowych w określonym celu, w określonym zakresie, przez określonego administratora danych osobowych. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. 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) przepis innej ustawy zezwala 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. Administrator Bezpieczeństwa Informacji prowadzi wykaz zbiorów danych osobowych zwany dalej wykazem zbiorów zgodnie ze wzorem stanowiącym załącznik nr 6 do niniejszej Polityki.

2. Zabrania się przetwarzania danych osobowych w zbiorach, które nie figurują w wykazie zbiorów.

3. Zabrania się przetwarzania danych osobowych w zbiorze, w stosunku do którego istnieje obowiązek zgłoszenia do rejestru GIODO przed dokonaniem tego zgłoszenia.

4. Zabrania się przetwarzania danych osobowych w zbiorach, zawierających dane osobowe wrażliwe przed dokonaniem rejestracji przez GIODO. Rejestracja takiego zbioru potwierdzona jest zaświadczeniem o zarejestrowaniu zbioru danych, które wydaje GIODO.

5. Zobowiązuje się kierowników referatów do informowania ABI o planowaniu utworzenia zbioru danych osobowych.

6. 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 powierzeniu przetwarzania.

7. Tworzenie nowego zbioru w systemie informatycznym może nastąpić tylko po uzgodnieniach z ASI i po akceptacji przez ABI.

8. Tworzenie nowego zbioru w formie dokumentu papierowego może nastąpić po akceptacji ABI.

9. W przypadku konieczności zarejestrowania nowego zbioru w rejestrze GIODO wniosek rejestracyjny w formie papierowej wypełnia MAI. MAI wypełnia wniosek od pkt 1 do pkt 16 w części dotyczącej środków ochrony fizycznej.

11. Wypełniony wniosek rejestracyjny przekazywany jest przez MAI do ASI, który w terminie do 7 dni uzupełnia go w zakresie dotyczącym opisu środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej oraz środków ochrony w ramach narzędzi programowych i baz danych.

12. ABI po uzupełnieniu wniosku w zakresie środków organizacyjnych, sprawdzeniu czy wszystkie wymagane elementy wniosku są wypełnione przesyła go do GIODO.

13. Dokumenty związane z rejestracją zbioru danych przechowuje Administrator Bezpieczeństwa Informacji.

14. Przetwarzanie danych osobowych w nowym zbiorze danych osobowych może nastąpić dopiero po zgłoszeniu zbioru danych osobowych do rejestru prowadzonego przez GIODO lub w przypadku danych osobowych wrażliwych po jego zarejestrowaniu.

15. W przypadku zamiaru przyjęcia zbioru danych osobowych w wyniku zawarcia umowy o powierzeniu przetwarzania danych lub w przypadku zamiaru przekazania zbioru danych osobowych do przetwarzania podmiotowi zewnętrznemu MAI realizujący to zadanie zobowiązany jest niezwłocznie przekazać projekt umowy do Administratora Bezpieczeństwa Informacji w celu jego uzgodnienia.

§ 6.

1. MAI przekazuje niezwłocznie do ABI informacje aktualizujące opis zbioru danych osobowych w wykazie zbiorów danych osobowych.

2. Aktualizacji zgłoszeń w rejestrze GIODO wymagają w szczególności następujące sytuacje:

   a) dokonanie zmian w warunkach technicznych związanych ze zgłoszonym zbiorem danych osobowych, wpływających na zmianę treści zgłoszenia,

   b) dokonanie zmian w warunkach organizacyjnych związanych ze zgłoszonym zbiorem danych osobowych, wpływających na zmianę treści zgłoszenia,

   c) zmiana podstaw prawnych lub celu przetwarzania danych osobowych ,

   d) zmiana zakresu przetwarzanych danych osobowych oraz zmiana kategorii osób, których dane dotyczą,

   e) zmiana odbiorców lub kategorii odbiorców, którym dane mogą być przekazywane,

   f) zmiana sposobu zbierania oraz udostępniania danych osobowych.

3) W przypadku konieczności aktualizacji zgłoszenia w rejestrze GIODO w związku z sytuacją określoną ust. 2 pkt b- f potrzebę w tym zakresie zobowiązany jest zgłosić niezwłocznie MAI do ABI. Procedura aktualizacji zgłoszenia zbioru do GIODO odpowiada procedurze zgłoszenia zbioru do rejestracji opisanej w § 5.

4) W przypadku zmian środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej lub środków ochrony w ramach narzędzi programowych i baz danych potrzebę dokonania aktualizacji

zgłoszenia zbioru do GIODO określa ASI. Jeśli konieczna jest aktualizacja zgłoszenia wówczas ASI wypełnia wniosek aktualizacyjny i przesyła do ABI, który dokonuje aktualizacji w rejestrze GIODO.

5) Zabrania się dokonywania zmian warunków technicznych i organizacyjnych związanych z ochroną danych osobowych bez konsultacji z ABI.

6) Zabrania się dokonywania zmian w zbiorze przetwarzanych danych osobowych, w przypadku gdy zmiana dotyczy rozszerzenia zakresu przetwarzania danych osobowych o dane osobowe wrażliwe przed zgłoszeniem tej zmiany do GIODO.

§ 7.

1. Działania związane z wyrejestrowaniem zbioru danych osobowych z rejestru GIODO podejmuje ABI na wniosek MAI.
2. Decyzja GIODO o wyrejestrowaniu zbioru danych jest podstawą wykreślenia zbioru z wykazu zbiorów.
3. W przypadku zbiorów danych, które nie są zarejestrowane przez GIODO, wykreślenie z wykazu zbiorów dokonuje ABI na wniosek MAI.
4. W przypadku wykreślenia z wykazu zbioru danych, który do przetwarzania danych osobowych wykorzystywał system informatyczny ASI podejmuje działania w celu zapewnienia komisyjnego fizycznego usunięcia zbiorów danych osobowych w formie elektronicznej z uwzględnieniem wymogów przepisów o archiwizacji danych. W skład komisji wchodzi MAI i ASI oraz pracownik merytoryczny. Pracami Komisji zarządza ASI, który informację o usunięciu zbioru przekazuje ABI.

§ 8.

1. W uzasadnionych przypadkach dopuszcza się powierzenie przetwarzania danych osobowych administrowanych przez Urząd podmiotowi zewnętrznemu.
2. Powierzenie przetwarzania danych odbywa się w drodze umowy zawartej na piśmie.
3. MAI jest zobowiązany do określenia zasad powierzenia w umowie. Jej treść musi obejmować co najmniej:
   a) zakres i cel przetwarzania danych osobowych,
   b) zobowiązanie podmiotu, któremu powierza się dane, do zastosowania środków zabezpieczających dane osobowe, o których mowa w art. 36 – 39 ustawy,
   c) oświadczenie o spełnieniu wymagań , o których mowa w art. 39a ustawy,
   d) określenie sposobu sprawowania przez Urząd kontroli należytego wykonania umowy w powyższym zakresie,
   e) określenie sposobu dochodzenia roszczeń przez Urząd w przypadku, gdy nastąpi naruszenie ochrony danych osobowych z przyczyn leżących po stronie podmiotu, któremu powierzono przetwarzanie danych osobowych.
4. MAI jest zobowiązany przekazać kopię umowy do Administratora Bezpieczeństwa Informacji.

## Rozdział 4.
## Opis zdarzeń naruszających ochronę danych osobowych

§ 9.

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 osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu,

c) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe lub osób odpowiedzialnych za ich ochronę.

2. Za naruszenie ochrony danych osobowych uważa się w szczególności:

a) przetwarzanie danych osobowych bez właściwego upoważnienia,

b) przetwarzanie danych osobowych z naruszeniem zasad opisanych w § 3,

c) przetwarzanie danych osobowych w zbiorach nieujętych w wykazie zbiorów,

d) brak możliwości fizycznego dostępu do danych w wyniku np. zagubionego klucza do pomieszczenia, lub mebli biurowych, w których przechowywane są dokumenty, zniszczonej szafy z dokumentami, braku nośników informacji itp.,

e) brak dostępu do zawartości zbioru danych pomimo, że zbiór istnieje,

f) zmienioną w sposób nieuprawniony zawartość zbioru, niepoprawną treść, postać, datę, różnicę w danych itp.,

g) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia, w którym jest przetwarzany,

h) zniszczenie lub próby zniszczenia w sposób nieautoryzowany danych ze zbioru lub danych systemowych,

i) zmianę lub utratę danych zapisanych na kopiach zapasowych lub zapisach archiwalnych,

j) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (dyskietki, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione,

k) próba nielegalnego logowania się do systemu lub włamania do systemu,

l) zmienione oprogramowanie systemu, stwierdzone przez użytkownika.

**§ 10.**

Zakazuje się przekazywania danych osobowych przez łącza teleinformatyczne niezabezpieczone.

## Rozdział 5.
## Zasady postępowania w sytuacji naruszenia ochrony danych osobowych

**§ 11.**

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz ABI lub osobę wskazaną przez ABI.

2. Użytkownik do momentu przybycia ABI lub osoby przez niego wskazanej 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, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych.

3. Po przybyciu na miejsce osoby, o której mowa w ust. 2 realizuje ona czynności w kolejności:

a) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych;

b) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia;

c) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony;

d) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń;

e) biorąc pod uwagę skalę oraz skutki naruszenia ochrony, ABI uruchamia doraźny zespół, w skład którego wchodzą ASI, MAI, osoba odpowiedzialna za administrowanie danym obiektem. ABI powiadamia o zdarzeniu Administratora lub osobę upoważnioną przez niego oraz o podjętych działaniach.

4. ABI z zastrzeżeniem ust. 7 z przebiegu zdarzenia sporządza raport z naruszenia bezpieczeństwa przetwarzania danych osobowych, który przekazuje Administratorowi lub osobie przez niego upoważnionej.

5. Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowanie przetwarzania danych wyraża ASI.

6. Dokonywanie zmian w miejscu naruszenia ochrony bez zgody ABI jest dopuszczalne tylko w wypadku konieczności ratowania osób, mienia albo zapobieżenia powstaniu innego niebezpieczeństwa.

7. W przypadku powołania doraźnego zespołu pracą jego kieruje ABI natomiast gdy naruszenie ochrony nastąpi w systemie informatycznym pracą zespołu kieruje ASI. Zespół sporządza raport, w którym ujmuje skalę stwierdzonych naruszeń ochrony, przyczyny ich powstania oraz skutki. Protokół zawierać powinien wnioski określające zakres działań organizacyjnych i technicznych, zapobiegających w przyszłości naruszeniom ochrony danych osobowych. Protokół przekazywany jest Administratorowi w celu akceptacji wniosków i zaleceń usprawniających ochronę danych.

## Rozdział 6.
## Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

### § 12.

1. W Urzędzie obowiązujące zasady użytkowania systemów informatycznych służących do przetwarzania danych osobowych określa Instrukcja.

2. Instrukcja, o której mowa w ust. 1 jest opracowywana przez ASI i następnie zatwierdzana przez Administratora. ASI wdraża Instrukcję do użytku w Urzędzie.

### § 13.

1. Dane osobowe w Urzędzie mogą być przetwarzane tylko przez osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych. Upoważnienie określa zakres uprawnień do wykonywania operacji na danych osobowych.

2. W Urzędzie prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
3. Zadanie prowadzenia ewidencji, o której mowa w ust. 2 realizuje Administrator Bezpieczeństwa Informacji. Ewidencja może być prowadzona w postaci elektronicznej.
4. Ewidencja, o której mowa w ust. 2 powinna zawierać:
   a) numer porządkowy,
   b) imię i nazwisko użytkownika,
   c) nazwę komórki organizacyjnej, w której jest zatrudniony,
   d) datę nadania upoważnienia do przetwarzania danych,
   e) zakres upoważnienia do przetwarzania danych osobowych,
   f) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym,
   g) datę ustania upoważnienia do przetwarzania danych osobowych,
   h) nr i datę wydania zaświadczenia o odbyciu szkolenia w zakresie ochrony danych osobowych lub datę podpisania oświadczenia, o którym mowa w § 14 ust. 11.
5. Zmiana informacji wyszczególnionych w ewidencji podlega niezwłocznemu odnotowaniu.

**§ 14.**

1. Upoważnienie do przetwarzania danych osobowych dla pracowników Urzędu wydawane jest, z zastrzeżeniem § 29, po złożeniu wniosku przez kierownika referatu lub jego przełożonego do ABI o udzielenie wskazanej osobie upoważnienia do przetwarzania danych osobowych. We wniosku określany jest zakres uprawnień do przetwarzania danych osobowych, który uwzględnia zakres realizowanych zadań.
2. Wzór wniosku o upoważnienie do przetwarzania danych osobowych zawiera załącznik nr 1 do Polityki.
3. Wzór upoważnienia do przetwarzania danych osobowych w Urzędzie zawiera załącznik nr 5 do Polityki.
4. Projekt upoważnienia opracowuje Administrator Bezpieczeństwa Informacji. Administrator może upoważnić ABI do podpisywania upoważnień do przetwarzania danych osobowych.
5. Upoważnienie do przetwarzania danych osobowych jest rejestrowane przez Administratora Bezpieczeństwa Informacji w ewidencji osób upoważnionych do przetwarzania danych osobowych.
6. W przypadku upoważnienia do przetwarzania danych osobowych w systemie informatycznym informacja ta przekazywania jest również do ASI w celu zapewnienia zarejestrowania użytkownika w systemie. Procedura związana z rejestracją użytkownika w systemie informatycznym jest określona w Instrukcji.
7. W przypadku potrzeby zmiany zakresu uprawnień do przetwarzania danych osobowych konieczne jest ponowne złożenie wniosku. Upoważnienie o zmienionym brzmieniu rejestrowane jest w ewidencji osób upoważnionych do przetwarzania danych osobowych.
8. Upoważnienie wykonywane jest w dwóch egzemplarzach, jeden przechowywany jest w komórce kadrowej drugi u Administratora Bezpieczeństwa Informacji.
9. Upoważnienie dla osoby, o której mowa w ust. 1 wydawane jest po podpisaniu przez nią oświadczenia o zobowiązaniu się do zachowania w tajemnicy, także po ustaniu realizacji zadań, poznanych danych

osobowych oraz informacji związanych z funkcjonowaniem systemu ochrony danych osobowych. Upoważnienie to jest ważne na czas realizacji zadań ustalonych z Administratorem.

10. Wzór oświadczenia, o którym mowa w ust. 9 zawiera załącznik nr 4 do Polityki.

11. Upoważnienia i oświadczenia, o którym mowa w ust. 9 wykonywane są w dwóch egzemplarzach. Odpowiednio jeden przechowuje właściwa merytorycznie jednostka organizacyjna, drugi przechowywany jest u Administratora Bezpieczeństwa Informacji.

12. Nadzór nad przestrzeganiem zasad ochrony danych osobowych przez osobę, o której mowa w ust. 1 realizuje właściwy merytorycznie kierownik referatu Urzędu.

**§ 15.**

Kierownik referatu po otrzymaniu informacji, o której mowa w § 14 ust. 7 zapewnia niezwłoczne uzupełnienie zakresu czynności właściwego użytkownika o czynności określone w otrzymanym przez niego upoważnieniu do przetwarzania danych osobowych oraz oświadczenia, o którym mowa w § 30 ust. 7. Opracowanie zakresu czynności odbywa się zgodnie z zasadami określonymi w Regulaminie Organizacyjnym Urzędu Miejskiego w Orzyszu.

**§ 16.**

1. Użytkownik traci aktualne upoważnienie do przetwarzania danych osobowych w sytuacjach:
   a) ustania zatrudnienia użytkownika u Administratora,
   b) zmiany zakresu obowiązków użytkownika,
   c) ustania wykonywania zadań przez osoby nie będące pracownikami Urzędu w związku z którymi otrzymały upoważnienia.
2. Przełożeni użytkowników zobowiązani są do niezwłocznego przekazywania informacji ABI w przypadku zaistnienia okoliczności powodujących utratę upoważnienia lub do ASI i ABI jeśli upoważnienie to dotyczy przetwarzania danych osobowych w systemie informatycznym.
3. Stanowisko ds. kadr niezwłocznie przekazuje informacje do Administratora Bezpieczeństwa Informacji oraz do Administratora Systemu o ustaniu zatrudnienia pracownika w Urzędzie jak również o przeniesieniu pracownika w strukturze Urzędu. Informację taką należy przekazać również w przypadku posiadania wiedzy o planowaniu wcześniej wymienionych zdarzeń.
4. W przypadku, gdy upoważnienie dotyczy przetwarzania danych osobowych w systemie informatycznym wyrejestrowanie z systemu następuje zgodnie z Instrukcją .
5. Ustanie upoważnienia odnotowywane jest w ewidencji osób upoważnionych do przetwarzania danych osobowych.

**§ 17.**

W przypadku przetwarzania danych osobowych w systemie informatycznym poza zbiorem danych i ograniczonego do edycji tekstu w celu udostępnienia go na piśmie po osiągnięciu celu przetwarzania należy je usunąć lub poddać animizacji.

**§ 18.**

W przypadku zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych po ich wykorzystaniu należy je niezwłocznie usunąć lub poddać animizacji.

§ 19.

Wszystkie osoby wykonujące zadania związane z przetwarzaniem danych osobowych zobowiązane są do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu wykonywania tych zadań.

§ 20.

1. Dane osobowe przetwarza się w budynkach, pomieszczeniach lub częściach pomieszczeń, tworzących obszar przetwarzania danych osobowych, który określany jest przez Administratora lub osobę przez niego upoważnioną.
2. Wykaz obiektów, pomieszczeń lub części pomieszczeń tworzących obszar przetwarzania danych osobowych stanowi załącznik nr 6 do Polityki.
3. Przebywanie osób trzecich w pomieszczeniach, w którym są przetwarzane dane osobowe jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
4. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe są zamykane na czas nieobecności użytkowników, uniemożliwiając do nich dostęp.
5. Zasady zabezpieczenia pomieszczeń i budynków po zakończeniu pracy określają właściwe instrukcje.
6. Instrukcje, o których mowa w ust. 5 określają zasady otwierania i zamykania budynków oraz pomieszczeń a także zasady ich sprzątania.

§ 21.

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonanie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do przetwarzania danych.
2. Zasady tworzenia kopii zapasowych oraz ich przechowywania określa Instrukcja.

§ 22.

Administrator może wyznaczyć zastępcę ABI, który współrealizuje zadania z zakresu ochrony danych osobowych .

§ 23.

1. Codzienną kontrolę bezpieczeństwa przetwarzania danych osobowych sprawują użytkownicy oraz ich przełożeni. Okresową kontrolę sprawują ASI oraz ABI.
2. Kierownik referatu Urzędu odpowiedzialny jest za prowadzenie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane. Okresowo powyższą kontrolę wykonuje ASI.
3. ABI opracowuje roczny plan kontroli w zakresie ochrony danych osobowych, który zatwierdza Administrator.
4. ASI opracowuje roczny plan kontroli w zakresie ochrony danych osobowych w systemach informatycznych urzędu, który zatwierdza Administrator.
5. ABI przeprowadza roczny audyt bezpieczeństwa zgodnie z planem stanowiącym załącznik nr 8 do niniejszej Polityki.

§ 24.

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu danych, w sposób uniemożliwiający ich odzyskanie,
   c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.
2. W celu zapewnienie 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 zasilacze awaryjne UPS.
4. W celu zapewnienia ochrony przed utratą danych stosuje się zasilacze awaryjne UPS przy stacjach roboczych odpowiednio do potrzeb. Konieczność takiego rozwiązania zgłasza MAI do ASI.

§ 25.

1. Systemy informatyczne służące do przetwarzania danych osobowych muszą być wyposażone w mechanizmy kontroli dostępu do tych danych.
2. Środki stosowane do uwierzytelniania w systemie informatycznym oraz zarządzanie identyfikatorami i hasłami określa Instrukcja.
3. Hasło podlega szczególnej ochronie, zakazuje się użytkownikowi jego udostępnianiu innym osobom. Przełożeni, osoby dokonujące przeglądów i konserwacji jak i innych prac związanych z systemem informatycznym muszą posiadać upoważnienia oraz własne identyfikatory i hasła umożliwiające dostęp do systemów informatycznych.

§ 26.

1. Użytkownicy systemów przetwarzających dane osobowe 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 osobowe wyposażone są w mechanizmy ochrony antywirusowej. Stosowanie tych mechanizmów oraz ich skuteczność kontroluje ASI.
3. Zasady ochrony antywirusowej określa Instrukcja.
4. W Urzędzie systemy posiadają zabezpieczenie przed działaniem oprogramowania mającego na celu uzyskanie nieuprawnionego dostępu do tych systemów. Za stosowanie tych zabezpieczeń odpowiada ASI.

§ 27.

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

§ 28.

ASI zapewnia aby system informatyczny, w którym przetwarzane są dane osobowe – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu

w celu udostępnienia go na piśmie – dla każdej osoby, której dane są przetwarzane odnotowywał w sposób automatyczny po zatwierdzeniu przez użytkownika operacji wprowadzenia danych oraz umożliwiał sporządzenie i wydrukowanie raportu w powszechnie zrozumiałej formie zawierającej:

1) datę pierwszego wprowadzenia danych do systemu,

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jeden użytkownik,

3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,

4) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

**§ 29.**

Osoba użytkująca komputer przenośny zawierający dane osobowe musi zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych. Rodzaj oprogramowania służącego do ochrony kryptograficznej ustala z ASI.

**§ 30.**

1. Użytkownicy zapoznają się z przepisami o ochronie danych osobowych.
2. Pracownik urzędu, który planowany jest do realizacji zadań związanych z przetwarzaniem danych osobowych odbywa szkolenie organizowane przez ABI w ramach procesu uzyskiwania pierwszego upoważnienia do przetwarzania danych osobowych.
3. Użytkownik odbywa obowiązkowo szkolenie w zakresie ochrony danych osobowych nie rzadziej niż co 5 lat.
4. Kierownik jednostki organizacyjnej odpowiada za umożliwienie udziału pracownika w szkoleniach o którym mowa w ust. 2 i ust. 3.
5. Za organizację szkolenia, o którym mowa w ust. 3 odpowiada ABI. W tym celu:
   a) ustala skład grupy szkolonych użytkowników w porozumieniu z kierownikami referatów Urzędu,
   b) opracowuje program szkolenia w zakresie ochrony danych osobowych, który zatwierdzany jest przez Administratora.
6. ABI wydaje zaświadczenie o odbyciu szkolenia. Wzór zaświadczenia zawiera załącznik nr 2 do Polityki bezpieczeństwa. Zaświadczenie przechowywane jest w komórce kadrowej. Administrator Bezpieczeństwa Informacji prowadzi wykaz pracowników przeszkolonych w zakresie ochrony danych osobowych.
7. Pracownik podpisuje oświadczenie o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych. Wzór oświadczenia zawiera załącznik nr 3 do Polityki bezpieczeństwa. Oświadczenie wykonywane jest w dwóch egzemplarzach. Jeden przechowywany jest w komórce kadrowej, drugi przechowywany jest u Administratora Bezpieczeństwa Informacji.

## Rozdział 7.
## Przepisy końcowe

### § 31.

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który stanowi załącznik nr 6 do Polityki. Wykaz prowadzi ABI.
2. Opis sposobu przepływu danych między systemami informatycznymi prowadzi ASI. ASI aktualizuje opis i przekazuje go do Administratora Bezpieczeństwa Informacji

Załącznik Nr 1 do „Polityki bezpieczeństwa Urzędu Miejskiego w Orzyszu."

Orzysz, .....

**Administrator Bezpieczeństwa Informacji**
**w/m**

**w n i o s k u j ę o udzielenie**

**Pani /Panu/** .....**

upoważnienia do przetwarzania danych osobowych w:

.....
(nazwa jednostki organizacyjnej Urzędu, nazwa komisji, itp.)

z powodu:/przyjęcia do pracy, przejścia na inne stanowisko, zmiany zakresu czynności/* lub innego (jakiego?): .....

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, lub jego przełożonego)

---

/* właściwe podkreślić

/** właściwe skreślić

Załącznik Nr 2 do „Polityki bezpieczeństwa Urzędu Miejskiego w Orzyszu."

**ZAŚWIADCZENIE NR .....**

**stwierdzające odbycie szkolenia**

**w zakresie ochrony danych osobowych**

Stwierdza się, że Pani (Pan):

.....

odbyła (odbył) szkolenie w zakresie ochrony danych osobowych wymagane przez „Politykę bezpieczeństwa dotyczącą sposobu przetwarzania danych osobowych w Urzędzie **Miejskim w Orzyszu"** zorganizowane przez administratora bezpieczeństwa informacji w:

**Urzędzie Miejskim w Orzyszu**

.....
(miejscowość i data)

.....
(podpis i imienna pieczątka administratora bezpieczeństwa informacji)

Załącznik Nr 3 do „Polityki bezpieczeństwa Urzędu Miejskiego w Orzyszu"

.....
(imię i nazwisko pracownika)

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

# O Ś W I A D C Z E N I E

**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. Nr 101 poz. 926 z późniejszymi zmianami).
2. Rozporządzenia 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 Miejskim w Orzyszu.**
4. Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie **Miejskim w Orzyszu.**

**<u>Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:</u>**

1) zapewnienia ochrony danych osobowych przetwarzanych w **Urzędzie Miejskim w Orzyszu**, 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 Miejskim w Orzyszu,**
3) zachowania w tajemnicy hasła dostępu do systemów informatycznych, przetwarzających dane osobowe w **Urzędzie Miejskim w Orzyszu**, 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 pracownika)

Załącznik Nr 4 do „Polityki bezpieczeństwa Urzędu Miejskiego w Orzyszu"

Orzysz, dnia .....

.....
(imię i nazwisko)

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

# O Ś W I A D C Z E N I E

**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. Nr 101 poz. 926 z późniejszymi zmianami).
2. Rozporządzenia 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 zobowiązuję się do:**

1) zapewnienia ochrony danych osobowych przetwarzanych w Urzędzie **Miejskim w Orzyszu**, 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 ABI próby lub faktu naruszenia bezpieczeństwa danych osobowych.

.....
(podpis)

Orzysz, dnia .....

Załącznik Nr 5 do „Polityki bezpieczeństwa
Urzędu Miejskiego w Orzyszu"

Orzysz, dnia .....

# U P O W A Ż N I E N I E

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)

wyłącznie w celu wynikającym z Pani/Pana zadań służbowych oraz poleceń przełożonego.

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

.....

(Administrator Danych Osobowych)

---

/* niepotrzebne skreślić
/** właściwe podkreślić

Załącznik Nr 6 do „Polityki bezpieczeństwa
Urzędu Miejskiego w Orzyszu"

## WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH (wzór)

| L.p. | Nazwa zbioru danych | Nazwa programu zastosowanego do przetwarzania danych osobowych |
|---|---|---|
| REFERAT OGÓLNOORGANIZACYJNY | | |
| | | |
| | | |
| REFERAT SPRAW OBYWATELSKICH/USC | | |
| | | |
| | | |
| REFERAT FINANSOWY | | |
| | | |
| | | |
| REFERAT SPRAW SPOŁECZNYCH I PROMOCJI | | |
| | | |
| | | |
| REFERAT SPRAW GOSPODARKI KOMUNALNEJ | | |
| | | |
| | | |
| REFERAT INWESTYCJI I ROZWOJU GOSPODARCZEGO | | |
| | | |
| | | |

## OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI (wzór)

### OR – Referat Ogólnoorganizacyjny

1) *nazwa zbioru z wykazu*
Dane osobowe: *np.*

1. *Nazwisko i imię*
2. *Adres zamieszkania/pobytu/do korespondencji.*
3. *NIP*

4. *PESEL*

Inne dane osobowe: *np. adres e-mail.*

# Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

| Lp. | Nr pokoju | Określenie w strukturze organizacyjnej urzędu | Uwagi |
|---|---|---|---|
| **Budynek Urzędu Miejskiego w Orzyszu** | | | |
| Parter wysoki | | | |
| 1 | 1 | Sala konferencyjna | OR |
| 2 | 2 | Biuro Rady | OR |
| 3 | 3 | Biuro Obsługi Rady | OR |
| 4 | 4 | Biuro Obsługi Interesanta | OR |
| 5 | 5 | USC | OS |
| 6 | 6 | Ewidencja ludności | OS |
| Półpiętro I | | | |
| 7 | 11 | Kierownik Referatu Inwestycji i Rozwoju Gospodarczego | RGI |
| 8 | 12 | Referat Inwestycji i Rozwoju Gospodarczego | RGI |
| 9 | 13 | Realizacja projektów z fin. zewnętrznym | RGI |
| Piętro I | | | |
| 10 | 21 | Sekretariat Burmistrza | OR |
| 11 | 22 | Sekretarz | OR |
| 12 | 23 | Skarbnik | FN |
| 13 | 24 | Kadry | OR |
| 14 | 25 | Podatki | FN |
| 15 | 26 | z-ca Skarbnika | FN |
| 16 | 27 | Kasa | FN |
| 17 | 28 | Windykacja, płace | FN |
| Półpiętro II | | | |
| 18 | 31 | Kierownik referatu spraw społecznych | SP |
| 19 | 32 | Rozwiązywanie problemów alkoholowych | SP |
| 20 | 33 | Promocja | SP |
| 21 | 34 | Egzekucja dłużników alimentacyjnych | SP |
| Piętro II | | | |
| 22 | 41 | Sekretariat Z-cy Burmistrza | OR |
| 23 | 42 | Pokój narad | OR |
| 24 | 43 | Zarządzanie Kryzysowe | OR |
| 25 | 44 | Informatyk | OR |
| 26 | 45 | Serwerownia | OR |
| 27 | 46 | Kierownik Referatu Komunalnego | GKR |
| 28 | 47 | Gospodarka mieszkaniowa | GKR |
| 29 | 48 | Gospodarka nieruchomościami | GKR |
| 30 | 49 | Ochrona środowiska i drogi | GKR |

Załącznik Nr 2 do Zarządzenia Nr 223/2012
Burmistrza Orzysza
z dnia 31.10.2013 r.

# INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU MIEJSKIEGO W ORZYSZU

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 Miejski w Orzyszu,
2. Administratorze Danych - należy przez to rozumieć Burmistrza Orzysz,
3. Administratorze Bezpieczeństwa Informacji - należy przez to rozumieć pracownika Urzędu lub inną 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,
3. Użytkowniku systemu - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu. Użytkownikiem może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy o pracę, powołania lub wyboru
5. Sieci lokalnej - należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
6. Sieci rozległej - należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, 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:
   1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.),
   2) Polityką bezpieczeństwa dotyczącą przetwarzania danych osobowych w Urzędzie Miejskim w Orzyszu
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 3 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 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:

    a. minimalna długość hasła - 8 znaków,

    b. zakazuje się stosować:

    - haseł, które użytkownik stosował uprzednio w okresie minionego kwartału,

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

    - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, imion dzieci i ich dat urodzenia 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 zabrania się z korzystania 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:

    Administrator Bezpieczeństwa Informacji

    Kierownik Urzędu lub osoba przez niego wyznaczona

## 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 komputerowe 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 stacja roboczych, na których przetwarzane są dane osobowe wprowadza się wysoki poziom zabezpieczeń.
2. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu 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 zainstalowany 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 dyskietkach, 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.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
6. 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.

B. Wydruki

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

## Rozdział 7.
## Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

1. Na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe, antyspamowe, pracujące w trybie monitora.
2. Każda poczta e-mail przychodząca do Urzędu musi być sprawdzona pod kątem występowania wirusów, spamu.
3. Definicje wzorców wirusów muszą być aktualizowane codziennie.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnika zamierza użyć.
5. Zabrania się pobierania z 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 przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum co miesiąc.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie wymienne nośniki posiadane przez użytkownika. Sprawdzana jest także cała sieć Urzędu.

## Rozdział 8.
## Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.
4. Udostępnienie danych osobowych może nastąpić wyłącznie po przedstawieniu wniosku, którego wzór stanowi załącznik Nr 3 do niniejszej instrukcji.
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.

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.
## Sposób postępowania w sytuacji naruszenia ochrony danych osobowych

1. Sposób postępowania w sytuacji stwierdzenia naruszenia ochrony danych osobowych określa Rozdział 5 Polityki bezpieczeństwa dotyczącej przetwarzania danych osobowych w Urzędzie Miejskim w Orzyszu.

## 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. Administrator Bezpieczeństwa Informacji zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zalogowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję 3.
3. Wszystkie logi opisujące pracę systemu, logowanie użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na nośniku wymiennym.

C. Rejestracja działań konserwacyjnych, awarii oraz napraw.

1. Administrator Bezpieczeństwa Informacji prowadzi "Dziennik systemu informatycznego Urzędu Miejskiego w Orzyszu". Wzór i zakres informacji rejestrowanych w dzienniku określony jest w załączniku Nr 4.
2. Wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji lub osoby przez nich wyznaczone.

## Rozdział 11.
## Połączenie do sieci Internet

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

Załącznik nr 1 do „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Orzyszu"

Orzysz, dn.....

.....

(imię i nazwisko pracownika)

.....

(stanowisko)

.....

(wydział)

## Wniosek o rejestrację w systemie informatycznym

Proszę o rejestrację w/w pracownika w następującym systemie (systemach) informatycznym:

.....

.....

Zakres uprawnień w systemie:

.....

.....

Data uruchomienia konta w systemie:.....

.....

.....(podpis pracownika)

(podpis przełożonego)

**Wyrażam zgodę / Nie wyrażam zgody**

.....

(podpis Administratora Danych )

Nadano identyfikator: .....

.....

(podpis ABI)

.....

(podpis administratora systemu)

Załącznik nr 2 do „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Orzyszu"

**Rejestr użytkowników systemu informatycznego Urzędu Miejskiego w Orzyszu**

| Lp. | Imię i Nazwisko | Identyfikator | Data nadania uprawnień | Data odebrania uprawnień | Przyczyna odebrania uprawnień |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |
| 10 | | | | | |

Załącznik nr 3 do „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Orzyszu"

## WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do ..... (dokładne oznaczenie administratora danych)

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 albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. 29 ust. 1 ustawy o ochronie danych osobowych: ..... .....* ? ..... 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 .....

Jeżeli TAK, to zakreśl kwadrat literą "x".

☐ (miejsce na znaczki opłaty skarbowej)

.....

*(data, podpis i ew. pieczęć wnioskodawcy)*

Załącznik nr 4 do „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Orzyszu"

**DZIENNIK SYSTEMU INFORMATYCZNEGO URZĘDU MIEJSKIEGO W ORZYSZU**

| Lp. | Data wpisu | Opis zdarzenia | Wpisu dokonał (Imię, Nazwisko, Stanowisko) | Podpis |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |