BURMISTRZ
Miasta i Gminy Kunów

Zarządzenie Nr 60/15
Burmistrza Miasta i Gminy Kunów
z dnia 11.03.2015 r.

w sprawie: wdrożenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy w Kunowie.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.) oraz § 3 i § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024) – zarządzam co następuje:

§ 1.

Dla zapewnienia ochrony przetwarzanych danych osobowych wprowadza się do użytku służbowego **Politykę Bezpieczeństwa Przetwarzania Danych Osobowych** w brzmieniu stanowiącym załącznik Nr 1 do niniejszego zarządzenia.

§ 2.

Polityka ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym Urzędu Miasta i Gminy w Kunowie.

§ 3.

1. Zobowiązuje się wszystkich pracowników Urzędu Miasta i Gminy w Kunowie, do zapoznania się z treścią **Polityki**, w terminie dwóch tygodni od dnia wejścia w życie Zarządzenia oraz praktycznego wdrożenia określonych w niej zasad przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Kunowie.
2. Za wykonanie postanowień ust. 1 odpowiadają bezpośredni przełożeni.

§ 4.

Wykonanie Zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 5.

Zarządzenie wchodzi w życie z dniem podjęcia.

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik Nr 1
do Zarządzenia Nr 60/15
Burmistrza Miasta i Gminy w Kunowie
z dnia 11.03.2015

Zatwierdzam

.....

Burmistrz Miasta i Gminy Kunów

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy w Kunowie

Rozdział I

Postanowienia ogólne.

§ 1

1. Polityka bezpieczeństwa dotycząca przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Kunowie, zwana dalej **„Polityką"**, jest dokumentem, którego celem jest określenie podstawowych reguł dotyczących zapewnienia bezpieczeństwa w zakresie przetwarzania danych osobowych:
   1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
   2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
2. Urząd Miasta i Gminy w Kunowie, 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:
   1) przetwarzane zgodnie z prawem,
   2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane przetwarzaniu niezgodnemu z tymi celami,
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakim są przetwarzane,
   4) 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 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 (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.) oraz § 3 i § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024).
6. **Polityka** podlega okresowej aktualizacji, która jest realizowana przez Administratora Bezpieczeństwa Informacji.

§ 2

Ilekroć w **Polityce** jest mowa o:

1) Administratorze Danych Osobowych – zwanym dalej **ADO** należy przez to rozumieć Burmistrza Miasta i Gminy w Kunowie.
2) **Ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
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 skazań, 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 Miasta i Gminy w Kunowie.
7) **Instrukcji** – rozumie się przez to **Instrukcję Zarządzania Systemem Informatycznym**, która obowiązuje w Urzędzie Miasta i Gminy w Kunowie.
8) Administratorze Bezpieczeństwa Informacji, zwanym dalej **ABI** - należy przez to rozumieć osobę wyznaczoną przez **ADO** i odpowiedzialną za rejestrację zbiorów danych osobowych, 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) Administratorze Systemów Informatycznych, zwanym dalej **ASI** - należy przez to rozumieć osobę wyznaczoną przez **ADO**, której celem działania jest nadzorowanie, kontrolowanie zasad bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.
10) Użytkowniku - należy przez to rozumieć pracownika **Urzędu**, który posiada upoważnienie wydane przez **ADO** lub osobę upoważnioną przez niego i dopuszczoną, w zakresie w nim wskazanym do przetwarzania danych osobowych.
11) Identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
12) Haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
13) Osobie trzeciej – należy przez to rozumieć każdą osobę nieupoważnioną i przez to nieuprawnioną do dostępu do danych osobowych będących w posiadaniu **ADO.** Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez **ADO** podejmująca czynności w zakresie przekraczającym ramy jego upoważnienia.

14) 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.
15) Zabezpieczeniu systemu informatycznego – należy przez to rozumieć wdrożenie przez **ADO** stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.
16) 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.
17) Usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
18) Poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom (osobom).
19) Integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
20) 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).
22) 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 II
Zasady przetwarzania danych osobowych

§ 3

1. Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy:
    1) osoba, której dane dotyczą, wyrazi zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
    2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
    3) 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,

4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
5) jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez **ADO** 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:
   1) nazwie i siedzibie **ADO**,
   2) celu zbierania danych, a w szczególności o znanych lub przewidywanych odbiorcach danych osobowych,
   3) prawie dostępu do treści swoich danych oraz ich poprawiania,
   4) dobrowolności lub obowiązku podania danych osobowych, a jeżeli taki obowiązek istnieje o jego podstawie prawnej.
2. Przepisu ust. 1 nie stosuje się, jeżeli:
   1) przepis innej ustawy zezwala na przetwarzanie danych osobowych bez ujawniania faktycznego celu ich zbierania,
   2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

Rozdział III

Zarządzanie zbiorami danych osobowych

§ 5

1. **ABI** prowadzi i aktualizuje **Rejestr zbiorów danych przetwarzanych przez ADO**, z wyjątkiem zbiorów, o których mowa w art.43 ust. 1, zawierający nazwę zbioru oraz informacje o których mowa w art. 41 ust. 1 pkt 2-4a i 7 **Ustawy**, tzn:
   1) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku powierzenia przetwarzania danych podmiotowi, o którym mowa w art. 31 **Ustawy**, lub wyznaczenia podmiotu, o którym mowa w art. 31a, oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania,
   2) cel przetwarzania danych,
   3) opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych,

4) sposób zbierania oraz udostępniania danych,
5) informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane,
6) informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

2. Sposób prowadzenia rejestru zbioru danych powinien być zgodny z wydanym na podstawie art. 36 a ust. 9 pkt. 2 **Ustawy** rozporządzeniem ministra właściwego do spraw administracji publicznej.
3. Zabrania się przetwarzania danych osobowych w zbiorach, które nie zostały wykazane w **Rejestrze danych przetwarzanych przez ADO**.
4. W przypadku konieczności zarejestrowania w GIODO zbioru zawierającego dane osobowe wrażliwe, o których mowa w art. 27 ust. 1 **Ustawy,** wniosek rejestracyjny na platformie e-giodo wypełnia **ABI**.
5. **ABI** po uzupełnieniu wniosku w zakresie środków organizacyjnych, sprawdzeniu czy wszystkie wymagane elementy wniosku są wypełnione przesyła go do GIODO.
6. **ABI** przechowuje dokumenty związane z rejestracją zbioru danych przez GIODO.
7. 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.
8. Zobowiązuje się kierowników komórek organizacyjnych do informowania **ABI** o planowaniu utworzenia zbioru danych osobowych.
9. Utworzenie nowego zbioru danych osobowych może być wynikiem:
   1) realizacji nowego celu,
   2) zidentyfikowania zbioru, który nie został wpisany do rejestru zbiorów.,
   3) przyjęcia zbioru danych osobowych w wyniku zawarcia umowy o powierzeniu przetwarzania.
10. Tworzenie nowego zbioru w systemie informatycznym może nastąpić tylko po akceptacji przez **ABI i ASI**.
11. Tworzenie nowego zbioru w formie dokumentu papierowego może nastąpić po akceptacji **ABI.**
12. 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, **ADO** realizujący to zadanie zobowiązany jest niezwłocznie przekazać projekt umowy do **ABI** w celu jego uzgodnienia.

§ 6

1. **ADO** przekazuje niezwłocznie do **ABI** informacje aktualizujące opis zbioru danych osobowych w **Rejestrze zbiorów danych osobowych przetwarzanych przez ADO.**
2. Aktualizacji zgłoszeń w rejestrach zbiorów danych osobowych prowadzonych przez **ABI** i GIODO wymagają w szczególności następujące sytuacje:
   1) dokonanie zmian w warunkach technicznych związanych ze zgłoszonym zbiorem danych osobowych, wpływających na zmianę treści zgłoszenia,

2) dokonanie zmian w warunkach organizacyjnych związanych ze zgłoszonym zbiorem danych osobowych, wpływających na zmianę treści zgłoszenia,
3) zmiana podstaw prawnych lub celu przetwarzania danych osobowych ,
4) zmiana zakresu przetwarzanych danych osobowych oraz zmiana kategorii osób, których dane dotyczą,
5) zmiana odbiorców lub kategorii odbiorców, którym dane mogą być przekazywane
6) zmiana sposobu zbierania oraz udostępniania danych osobowych.

3. W przypadku konieczności aktualizacji zgłoszenia w rejestrach prowadzonych przez **ABI** i GIODO w związku z sytuacją określoną ust. 2 pkt 2- 6 potrzebę w tym zakresie zobowiązany jest zgłosić niezwłocznie **ADO** do **ABI**. Procedura aktualizacji zgłoszenia zbioru 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 **ABI** i GIODO określa **ASI**. Jeśli konieczna jest aktualizacja zgłoszenia wówczas **ASI** wypełnia wniosek aktualizacyjny i przekazuje go **ABI**, który dokonuje aktualizacji w prowadzonym przez siebie rejestrze lub zgłasza aktualizację do rejestru prowadzonego przez 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 prowadzonego przez siebie rejestru i rejestru GIODO podejmuje **ABI** na wniosek **ADO.**
2. Decyzja GIODO o wyrejestrowaniu zbioru danych jest podstawą do wykreślenia przez **ABI** tego zbioru z **Rejestru zbiorów danych osobowych przetwarzanych przez ADO.**
3. W przypadku zbiorów danych, które nie są zarejestrowane przez GIODO, wykreślenia z prowadzonego przez siebie rejestru dokonuje **ABI.**
4. W przypadku wykreślenia z rejestru 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.

§ 8

1. W uzasadnionych przypadkach dopuszcza się powierzenie przetwarzania danych osobowych administrowanych przez **ADO** podmiotowi zewnętrznemu.
2. Powierzenie przetwarzania danych odbywa się w drodze umowy zawartej na piśmie.
3. Projekt umowy przygotowuje **ABI**, a zatwierdza **ADO**.
4. **ADO** jest zobowiązany do określenia zasad powierzenia w umowie. Jej treść musi obejmować co najmniej:
   1) zakres i cel przetwarzania danych osobowych,

2) zobowiązanie podmiotu, któremu powierza się dane, do zastosowania środków zabezpieczających dane osobowe, o których mowa w art. 36, 37, 38 i 39 **Ustawy**,
3) oświadczenie o spełnieniu wymagań , o których mowa w art. 39a **Ustawy**,
4) określenie sposobu sprawowania przez **ADO** kontroli należytego wykonania umowy w powyższym zakresie,
5) określenie sposobu dochodzenia roszczeń przez **ADO** w przypadku, gdy nastąpi naruszenie ochrony danych osobowych z przyczyn leżących po stronie podmiotu, któremu powierzono przetwarzanie danych osobowych.

5. Kopię umowy przechowuje **ABI.**

Rozdział IV

Opis zdarzeń naruszających ochronę danych osobowych

§ 9

1. Naruszenie ochrony danych osobowych, może być spowodowane:
   1) niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, skutki powodzi, pożaru, itp.,
   2) 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,
   3) 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:
   1) przetwarzanie danych osobowych bez właściwego upoważnienia,
   2) przetwarzanie danych osobowych z naruszeniem zasad opisanych w § 3,
   3) przetwarzanie danych osobowych w zbiorach nieujętych w wykazie zbiorów,
   4) 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.,
   5) brak dostępu do zawartości zbioru danych pomimo, że zbiór istnieje,
   6) zmienioną w sposób nieuprawniony zawartość zbioru, niepoprawną treść, postać, datę, różnicę w danych itp.,
   7) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia w którym jest przetwarzany,
   8) zniszczenie lub próby zniszczenia w sposób nieautoryzowany danych ze zbioru lub danych systemowych,
   9) zmianę lub utratę danych zapisanych na kopiach zapasowych lub zapisach archiwalnych,
   10) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (dyskietki, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione,
   11) próba nielegalnego logowania się do systemu lub włamania do systemu,

12) zmienione oprogramowanie systemu, stwierdzone przez użytkownika.

§ 10

Zakazuje się przekazywania danych osobowych przez łącza teleinformatyczne niezabezpieczone.

Rozdział V

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 bezpośredniego przełożonego oraz **ABI.**
2. Użytkownik do momentu przybycia **ABI** powinien:
   1) zabezpieczyć dostęp do pomieszczenia lub urządzenia;
   2) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony;
   3) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony;
   4) 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:
   1) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych;
   2) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia;
   3) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony;
   4) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń i powiadamia o zdarzeniu **ADO**;
   5) w zależności od skali i skutków naruszenia ochrony **ABI** uruchamia doraźny zespół, w skład którego wchodzą **ASI i ADO** oraz osoba odpowiedzialna za administrowanie danym obiektem.
4. **ABI** z zastrzeżeniem ust. 7 z przebiegu zdarzenia sporządza raport z naruszenia bezpieczeństwa przetwarzania danych osobowych, który przekazuje **ADO.**
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 **ADO** w celu akceptacji wniosków i zaleceń usprawniających ochronę danych.

Rozdział VI

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

§ 12

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

§ 13

1. Dane osobowe w **Urzędzie** mogą być przetwarzane tylko przez osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez **ADO**. Upoważnienie określa zakres uprawnień do wykonywania operacji na danych osobowych.
2. W **Urzędzie** prowadzona jest **Ewidencja osób upoważnionych do przetwarzania danych osobowych,** którą przedstawia **Załącznik nr 1**.
3. Zadanie prowadzenia ewidencji, o której mowa w ust. 2 realizuje **ABI**.
4. Ewidencja o której mowa w ust. 2 powinna zawierać:
   1) numer porządkowy,
   2) imię i nazwisko użytkownika,
   3) nazwę komórki organizacyjnej, w której jest zatrudniony,
   4) datę nadania upoważnienia do przetwarzania danych,
   5) zakres upoważnienia do przetwarzania danych osobowych,
   6) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym,
   7) datę ustania upoważnienia do przetwarzania danych osobowych,
   8) 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 pracownika **Urzędu** wydawane jest, z zastrzeżeniem § 29, po złożeniu wniosku przez jego bezpośredniego przełożonego

do **ADO** poprzez **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. Upoważnienie do przetwarzania danych osobowych dla osoby nie będącej pracownikiem **Urzędu** następuje na wniosek właściwego merytorycznie kierownika komórki organizacyjnej, który składany jest do **ABI**. We wniosku określany jest zakres uprawnień do przetwarzania danych osobowych, który uwzględnia zakres realizowanych zadań.
3. Wzór wniosku o upoważnienie do przetwarzania danych osobowych zawiera **Załącznik nr 2.**
4. Wzór upoważnienia do przetwarzania danych osobowych w **Urzędzie** zawiera **Załącznik nr 3.**
5. Projekt upoważnienia opracowuje **ABI**. **ADO** może upoważnić **ABI** do podpisywania upoważnień do przetwarzania danych osobowych.
6. Upoważnienie do przetwarzania danych osobowych jest rejestrowane przez **ABI** w **Ewidencji osób upoważnionych do przetwarzania danych osobowych.**
7. Po wydaniu upoważnienia **ABI** przekazuje o tym informację przełożonemu pracownika, któremu wydano upoważnienie.
8. 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.**
9. 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.
10. Upoważnienie wykonywane jest w trzech egzemplarzach, jeden otrzymuje osoba ubiegająca się o upoważnienie, drugie przechowywane jest w jego aktach osobowych, a trzecie stanowi załącznik do **Ewidencji osób upoważnionych do przetwarzania danych osobowych** prowadzonej przez **ABI.**
11. Upoważnienie dla osoby, o której mowa w ust. 2 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 **ADO**.
12. Wzór oświadczenia, o którym mowa w ust. 11 zawiera **Załącznik nr 4.** .
13. Upoważnienia i oświadczenia, o którym mowa w ust. 11 wykonywane są w trzech egzemplarzach. Odpowiednio jeden egzemplarz otrzymuje upoważniona osoba, drugi odpowiedzialny za przetwarzany zbiór danych kierownik, trzeci przechowywany jest przez **ABI.**
14. Nadzór nad przestrzeganiem zasad ochrony danych osobowych przez osobę, o której mowa w ust. 2 realizuje właściwy merytorycznie kierownik odpowiedzialny za zbiór danych osobowych przetwarzanych przez tę osobę.

§ 15

Przełożony pracownika po otrzymaniu informacji, o której mowa w § 14 ust. 7 zapewnia w porozumieniu z **ADO** 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 Miasta i Gminy w Kunowie.

§ 16

1. Użytkownik traci aktualne upoważnienie do przetwarzania danych osobowych w sytuacjach:
   1) ustania zatrudnienia użytkownika u ADO,
   2) zmiany zakresu obowiązków użytkownika,
   3) ustania wykonywania zadań przez osoby nie będące pracownikami Urzędu w związku z którymi otrzymały upoważnienia.
2. Przełożeni użytkowników zobowiązani są do niezwłocznego przekazywania informacji **ADO** i **ABI** w przypadku zaistnienia okoliczności powodujących utratę upoważnienia lub do **ABI** i **ASI** jeśli upoważnienie to dotyczy przetwarzania danych osobowych w systemie informatycznym.
3. Informację, o której mowa w ust.2 w przypadku osoby nie będącej pracownikiem przekazuje właściwy merytorycznie kierownik odpowiedzialny za zbiór danych osobowych przetwarzanych przez osobę, o której mowa w § 14 ust. 2.
4. **ADO** niezwłocznie przekazuje do **ABI** informację o ustaniu zatrudnienia pracownika w **Urzędzie** jak również o przeniesieniu pracownika na inne stanowisko.
5. W przypadku, gdy upoważnienie dotyczy przetwarzania danych osobowych w systemie informatycznym wyrejestrowanie z systemu następuje zgodnie z **Instrukcją** .
6. 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 anonimizacji.

§ 18

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

§ 19

Wszystkie osoby wykonujące zadania związane z przetwarzaniem danych osobowych zobowiązane są do zachowania ich w tajemnicy. Tajemnica obowiązuje ich 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 **ABI.**
2. Wykaz obiektów, pomieszczeń lub części pomieszczeń tworzących obszar przetwarzania danych osobowych zawiera **Wykaz zbiorów danych osobowych** prowadzony przez **ABI,** który przedstawia **Załącznik nr 5.**
3. Przebywanie osób trzecich w pomieszczeniach, w którym są przetwarzane dane osobowe jest dopuszczalne za zgodą **ABI** 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.
5. Zasady zabezpieczenia pomieszczeń i budynków określają właściwe instrukcje opracowywane przez komórkę organizacyjną **Urzędu** odpowiedzialną za administrowanie jego obiektami. Instrukcje podlegają uzgodnieniu z **ABI,** a następnie zatwierdzane są przez **ADO.**
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

1. Codzienną kontrolę bezpieczeństwa przetwarzania danych osobowych sprawują użytkownicy oraz ich przełożeni. Okresową kontrolę sprawują **ASI** oraz **ABI.**
2. Kierownik komórki organizacyjnej **Urzędu,** w której przetwarzane są dane osobowe odpowiedzialny jest za prowadzenie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane.
3. Do kontroli stanu ochrony danych osobowych w Urzędzie Miasta i Gminy w Kunowie upoważnieni są: **ADO, ABI** i **ASI.**
4. Raz w roku kontroli podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe.
5. **ABI** wspólnie z **ASI** przygotowuje plan kontroli i jej zakres.
6. Kontroli podlega warstwa sprzętowa, systemy operacyjne, aplikacje, realizacja zabezpieczeń przez pracowników **Urzędu** oraz przestrzeganie polityki bezpieczeństwa.
7. Po dokonaniu kontroli sprawdzającej **ABI** zgodnie z art. 36a ust. 2 pkt 1 lit. a **Ustawy** opracowuje dla **ADO** sprawozdanie ze zgodności przetwarzania danych osobowych z przepisami o ich ochronie. Na jego podstawie **ADO** podejmuje właściwe działania

korygujące i doskonalące zabezpieczenie zbiorów danych osobowych przetwarzanych w **Urzędzie.**

8. Tryb i sposób wykonania ww. sprawozdania określi zgodnie z art. 36a ust.9 pkt.2 **Ustawy** rozporządzenie ministra właściwego do spraw administracji
9. Sprawozdanie, o którym mowa w art. 36a ust. 2 pkt 1 lit. a Ustawy powinno zawierać:
   1) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania;
   2) imię i nazwisko **ABI;**
   3) wykaz czynności podjętych przez **ABI** w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
   4) datę rozpoczęcia i zakończenia sprawdzenia;
   5) określenie przedmiotu i zakresu sprawdzenia;
   6) opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
   7) stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
   8) wyszczególnienie załączników stanowiących składową część sprawozdania;
   9) podpis **ABI**, a w przypadku sprawozdania w postaci papierowej - dodatkowo parafy **ABI** na każdej stronie sprawozdania;
   10) datę i miejsce podpisania sprawozdania przez **ADO.**

§ 23

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu danych, w sposób uniemożliwiający ich odzyskanie,
   3) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem **ASI.**
2. W celu zapewnienia nieprzerwanej i bezpiecznej pracy systemów informatycznych prowadzone są okresowe przeglądy i konserwacje, które zapewnia **ASI.** Zasady prowadzenia przeglądów i konserwacji urządzeń komputerowych, systemów informatycznych oraz zbiorów danych określa **Instrukcja.**
3. W celu zapewnienia ochrony serwerów przed utratą danych w wyniku awarii zasilania stosuje się zasilacze awaryjne UPS.
4. W celu zapewnienia ochrony przed utratą danych stosuje się zasilacze awaryjne UPS przy stacjach roboczych odpowiednio do potrzeb.

§ 24

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.

§ 25

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**.

§ 26

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

§ 27

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**.

§ 28

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**.

§ 29

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 komórki 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:
   1) ustala skład grupy szkolonych użytkowników w porozumieniu z kierownikami komórek organizacyjnych Urzędu,
   2) opracowuje program szkolenia w zakresie ochrony danych osobowych, który zatwierdzany jest przez **ADO**.
6. **ABI** wydaje zaświadczenie o odbyciu szkolenia. Wzór zaświadczenia zawiera **Załącznik nr 6.** Zaświadczenie wykonywane jest w dwóch egzemplarzach. Jeden otrzymuje przeszkolony pracownik, a drugi przechowywany jest w jego aktach osobowych. **ABI** prowadzi **Wykaz pracowników przeszkolonych w zakresie ochrony danych osobowych**, który przedstawia **Załącznik nr 7.**
7. Pracownik odbierając zaświadczenie podpisuje oświadczenie o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych. Wzór oświadczenia zawiera **Załącznik nr 8.** Oświadczenie wykonywane jest w trzech egzemplarzach. Jeden otrzymuje użytkownik, drugi przechowywany jest w jego aktach osobowych, a trzeci stanowi załącznik do **Wykazu pracowników przeszkolonych w zakresie ochrony danych osobowych.**

Rozdział VII

Przepisy końcowe

§ 30

1. **Wykaz zbiorów danych osobowych** wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe prowadzi **ABI**.
2. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, który stanowi **Załącznik nr 9** prowadzi **ABI.**

3. Opis sposobu przepływu danych między systemami informatycznymi, który stanowi **Załącznik nr 10** przygotowuje **ASI. ASI** aktualizuje opis i przekazuje go do **ABI.**

§ 31

1. Instrukcje, o których mowa w § 20 ust. 5 zostaną zaktualizowane lub opracowane i przedstawione do zatwierdzenia **ADO** w ciągu 30 dni od dnia wejścia w życie **Polityki Bezpieczeństwa Przetwarzania Danych Osobowych.**
2. Instrukcja, o której mowa w § 12 zostanie zaktualizowana i przedstawiona do zatwierdzenia **ADO** w ciągu 7 dni od dnia wejścia w życie **Polityki Bezpieczeństwa Przetwarzania Danych Osobowych.**
3. Opis, o którym mowa w § 30 ust. 3 zostanie opracowany przez **ASI** i przekazany do **ABI** w ciągu 30 dni od dnia wejścia w życie **Polityki Bezpieczeństwa Przetwarzania Danych Osobowych.**
4. **ABI** wprowadzi **Rejestr zbiorów danych przetwarzanych przez ADO** niezwłocznie po opublikowaniu rozporządzenia ministra właściwego do spraw administracji publicznej wydanego na podstawie art. 36 a ust. 9 pkt. 2 **Ustawy**, które określi sposób prowadzenia rejestru zbioru danych osobowych przez **ABI.**
5. **Polityka Bezpieczeństwa Przetwarzania Danych Osobowych** jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
6. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu traktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Postępowanie dyscyplinarne można wszcząć wobec osoby, która w przypadku naruszenia zabezpieczeń sytemu informatycznego lub uzasadnionego domniemania takiego naruszenia, nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła **ABI, ASI** lub **ADO**, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek.
7. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z **Ustawą** oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
8. Wszystkie regulacje dotyczące systemów informatycznych określone w **Polityce** dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
9. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej **Polityce.**
10. W sprawach nieuregulowanych w niniejszej **Polityce** mają zastosowanie przepisy **Ustawy** oraz wydane na jej podstawie akty wykonawcze.

Załączniki:

1. **Załącznik nr 1** – Ewidencja osób upoważnionych do przetwarzania danych osobowych
2. **Załącznik nr 2** – Wzór – Wniosek o upoważnienie do przetwarzania danych osobowych
3. **Załącznik nr 3** – Wzór – Upoważnienie do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Kunowie.
4. **Załącznik nr 4** – Wzór – Oświadczenie osoby nie będącej pracownikiem Urzędu.
5. **Załącznik nr 5** - Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.
6. **Załącznik nr 6** – Wzór – Zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony danych osobowych
8. **Załącznik nr 7** – Wykaz pracowników przeszkolonych w zakresie ochrony danych osobowych
9. **Załącznik nr 8** – Wzór – Oświadczenie pracownika Urzędu o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych.
10. **Załącznik nr 9** - Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.
11. **Załącznik nr 10** - Opis sposobu przepływu danych między systemami informatycznymi.

BURMISTRZ

mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 1
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w UMiG w Kunowie

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Nazwisko i imię	System informatyczny/ papierowy Nazwa aplikacji Nazwa zbioru danych osobowych	Zakres uprawnień	Data nadania upoważnienia	Data ustania upoważnienia
1					
2					
3					
4					
5					
6					
7					

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 2
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w UMiG w Kunowie

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 komórki organizacyjnej Urzędu, nazwa komisji, itp.)

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

Upoważnienie dotyczy:

1. **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/***
   .....
   .....
   .....
   .....
2. **Zakres uprawnień:** .....
   .....
   .....
3. **Sposób przetwarzania danych osobowych:** papierowy/ w systemie informatycznym/*
4. **Miejsce przetwarzania danych osobowych** (adres siedziby, piętro, nr pokoju)
   .....
   .....

.....
(pieczątka i podpis kierownika komórki organizacyjnej Urzędu, lub jego przełożonego)

/* właściwe podkreślić
/ właściwe skreślić**

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 3
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w UMiG w Kunowie

UPOWAŻNIENIE

NR .....

na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.).

upoważniam

Panią/ Pana* .....

do przetwarzania danych osobowych

w ramach .....

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

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

(systemu informatycznego, systemu w postaci papierowej)

w zakresie .....
.....

(nazwa uprawnień w zakresie przetwarzania danych)

Upoważnienie jest ważne w czasie zatrudnienia użytkownika u Administratora Danych Osobowych 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.

Kunów, dnia ....

.....
(Administrator Danych Osobowych)

/* niepotrzebne skreślić
/** właściwe podkreślić

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 4
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w UMiG w Kunowie

.....
(imię i nazwisko)

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

O Ś W I A D C Z E N I E

osoby nie będącej pracownikiem Urzędu

Oświadczam, że zobowiązuję się do przestrzegania:

1. **Ustawy z dnia 29 sierpnia 1997r.** o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.).
2. **Rozporządzenia Ministra Spraw Wewnętrznych i Administracji** z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100 poz. 1024),

Jednocześnie w czasie wykonywania swoich zadań zobowiązuję się do:

a) zapewnienia ochrony danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Kunowie, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom nieuprawnionym, zabraniem, uszkodzeniem oraz nieuprawnioną modyfikacją lub zniszczeniem,

b) zachowania w tajemnicy, także po ustaniu realizacji zadań poznanych danych osobowych oraz informacji związanych z funkcjonowaniem systemu ochrony danych osobowych.

c) zgłaszania Burmistrzowi Miasta i Gminy Kunów próby lub faktu naruszenia bezpieczeństwa danych osobowych.

Kunów, dnia .....

.....
(podpis)

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 5
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w UMiG w Kunowie

WYKAZ ZBIORÓW DANYCH OSOBOWYCH
wraz
ze wskazaniem programów zastosowanych do przetwarzania tych danych
oraz
budynków i pomieszczeń tworzących obszar,
w którym przetwarzane są dane osobowe

L.p.	Nazwa zbioru danych	Nazwa programu zastosowanego do przetwarzania danych osobowych	Obszar przetwarzania danych osobowych (np.: dane są przetwarzane na parterze budynku UMiG , w pokoju nr 8)	Adres
1				
2				
3				
4				
5				
6				
7				

BURMISTRZ
mgr Piotr Lodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 7
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w UMiG w Kunowie

WYKAZ PRACOWNIKÓW PRZESZKOLONYCH W ZAKRESIE OCHRONY DANYCH OSOBOWYCH BIORÓW DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Numer i data wydania zaświadczenia	Data złożenia oświadczenia pracownika Urzędu o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych
1			
2			
3			
4			
5			
6			
7			

BURMISTRZ
mgr Lech Sodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 8
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w UMiG w Kunowie

.....
(imię i nazwisko pracownika)

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

OŚWIADCZENIE

pracownika Urzędu o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych

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

1. **Ustawy z dnia 29 sierpnia 1997r.** o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.).
2. **Rozporządzenia Ministra Spraw Wewnętrznych i Administracji** z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100 poz. 1024),
3. **Polityki Bezpieczeństwa Przetwarzania Danych Osobowych** w Urzędzie Miasta i Gminy w Kunowie.
4. **Instrukcji Zarządzania Systemem Informatycznym**, służącym do przetwarzania danych w Urzędzie Miasta i Gminy w Kunowie.
5. **Instrukcji Zarządzania Systemem Informatycznym**, służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Kunowie.

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

a) zapewnienia ochrony danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Kunowie, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom nieuprawnionym, zabraniem, uszkodzeniem oraz nieuprawnioną modyfikacją lub zniszczeniem,
b) 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 Miasta i Gminy w Kunowie,
c) zachowania w tajemnicy hasła dostępu do systemów informatycznych, przetwarzających dane osobowe w Urzędzie Miasta i Gminy w Kunowie, również po upływie jego ważności,
d) 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.

Kunów, dn. .....

.....
(podpis pracownika)

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 9
do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych
w UMiG w Kunowie

OPIS STRUKTURY ZBIORÓW DANYCH OSOBOWYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

L.p.	Nazwa zbioru danych osobowych	Zawartość poszczególnych pól informacyjnych i powiązania między nimi
1.		**Zakres:**
2.		**Zakres:**
3.		**Zakres:**
4.		**Zakres:**
5.		**Zakres:**

BURMISTRZ
inż. Lech Łodej