Załącznik Nr 1 do Zarządzenia Burmistrza
Łobżenicy Nr 0050.58.2016 z dnia 23 czerwca 2016 r.

URZĄD MIEJSKI GMINY ŁOBŻENICA

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM GMINY ŁOBŻENICY

ZATWIERDZAM
BURMISTRZ
Piotr Łosoś (2)
.....

OPRACOWAŁ:

Administrator Bezpieczeństwa Informacji
w Urzędzie Miejskim Gminy w Łobżenicy

Łobżenica, dnia 23 czerwca 2016 roku.

POSTANOWIENIA OGÓLNE

§ 1. **Polityka bezpieczeństwa** została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 z późn, zm.) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024). Dokument został opracowany zgodnie z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 2. Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Urzędzie Miejskim Gminy w Łobżenicy.

§ 3. Ilekroć w Polityce jest mowa o :

1) **jednostka organizacyjna, Urzędzie** – rozumie się przez to Urząd Miejski Gminy w Łobżenicy;
2) **zbiorze danych osobowych** – 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;
3) **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) **przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
5) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
6) **systemie tradycyjnym** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;

7) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to drożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
8) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
9) **Administratorze Danych Osobowych** zwanym też **Administratorem Danych (ADO)** – w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Burmistrza Łobżenicy, który decyduje o celach i środkach przetwarzania danych osobowych;
10) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)** – rozumie się przez to osobę wyznaczoną przez Administratora Danych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
11) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** – rozumie się przez to osobę zatrudnioną przez Administratora Danych, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
12) **kierownik komórki organizacyjnej** – rozumie się również samodzielne stanowisko pracy,
13) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** – rozumie się przez to upoważnionego przez Administratora Danych, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony danych;
14) **zgodzie osoby, której te dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie - zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Rozdział I
CELE

§ 4. Dane osobowe w Urzędzie są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Urzędu na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

§ 5. Polityka bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się swoją treścią do informacji:

1) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
2) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

§ 6. Celem opracowania Polityki bezpieczeństwa jest ochrona danych osobowych przed niepowołanym dostępem do zgromadzonych i przetwarzanych danych.

§ 7. Procedury i zasady określone w niniejszej Polityce bezpieczeństwa stosuje się do wszystkich pracowników Urzędu, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Urzędzie (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, stażystów, praktykantów, serwisantów).

§ 8.1. Przetwarzanie danych osobowych do celów związanych z działalnością Administratora Danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.

2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, to ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.

3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.

4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji.

§ 9.1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych ustawą należy poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania,
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 10.1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3) źródle danych,
4) prawie dostępu do treści swoich danych oraz ich poprawiania,
5) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
6) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

2. Administrator Danych nakłada taki obowiązek na osoby zatrudnione przy przetwarzaniu danych osobowych.

Rozdział II
ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§ 11.1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych (ADO).

2. Kierownicy komórek organizacyjnych obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 12. Z polityką bezpieczeństwa danych osobowych w Urzędzie związane są następujące dokumenty:

1) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
2) Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.

§ 13.1. Każda osoba przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami w wersji papierowej winna zostać poddana przeszkoleniu lub zapoznana z:

1) przepisami ustawy o ochronie danych osobowych oraz przepisami wydanych do niej aktów wykonawczych,
2) zasadami ochrony danych osobowych zawartymi w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym.

2. Za organizację szkolenia lub zapoznania z zasadami ochrony danych osobowych odpowiada Administrator Bezpieczeństwa Informacji.

§ 14.1. Pracownicy zapoznani z zasadami ochrony danych osobowych zobowiązani są do podpisania Oświadczenia o poufności, którego wzór stanowi załącznik Nr 1 do Polityki bezpieczeństwa.

2. Oświadczenie przechowywane jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji ABI.

§ 15.1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy Urzędu posiadający imienne zarejestrowane Upoważnienie, którego wzór stanowi załącznik Nr 2 do niniejszej Polityki.

2. Upoważnienie określone w ust. 1 przechowywane jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji ABI.

§ 16.1. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji.

2. Wzór ewidencji określonej w ust. 2 stanowi załącznik Nr 3 do Polityki bezpieczeństwa.

§ 17. Administrator Danych Osobowych może powołać Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony, który prowadzi dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 18.1. Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

2. Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak by wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych i tradycyjnych.

3. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji jest następujący:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 ustawy o ochronie danych osobowych, oraz przestrzegania zasad w niej określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7.
3) nadzorowanie bezpieczeństwa systemów informatycznych i tradycyjnych;
4) nadzorowanie przestrzegania przez wszystkich użytkowników stosowania obowiązujących procedur;
5) dbanie, aby użytkownicy mający dostęp do systemu posiadali stosowne upoważnienia oraz byli przeszkoleni w zakresie obowiązujących regulacji bezpieczeństwa;
6) prowadzenie kontroli w zakresie bezpieczeństwa;
7) współdziałanie z Generalnym Inspektorem Ochrony Danych Osobowych w zakresie sprawdzeń zleconych przez GIODO
8) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych.

§ 19.1. Administrator Danych Osobowych wyznacza Administratora Systemu Informatycznego (ASI), który zapewnia prawidłowe działanie systemu informatycznego.

2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, w taki sposób, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.

3. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Systemu Informatycznego jest następujący:

1) zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora,
2) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego,
3) zakładanie kont oraz przydzielanie uprawnień upoważnionym użytkownikom,
4) wyrejestrowywanie użytkowników z systemu informatycznego,
5) prowadzenie ewidencji zarejestrowanych użytkowników systemu informatycznego, w których przetwarzane są dane osobowe,
6) nadzorowanie działań mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
7) instalowanie i usuwanie oprogramowania systemowego i narzędziowego,
8) odpowiada i sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;

9) wykonywanie kopii awaryjnych oraz nadzorowanie ich przechowywania,
10) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,
11) realizacja zadań związanych z przeszkoleniem użytkowników w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji , którą będą wykorzystywali.

§ 20. Kierownik komórki organizacyjnej odpowiada za przestrzeganie ustawy o ochronie danych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

1) kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników,
2) kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie,
3) zgłasza ABI rejestrację nowych zbiorów lub zmianę w obecnych zbiorach oraz przygotowuje wniosek w tej sprawie. Wzór wniosku stanowi załącznik Nr 4 do Polityki,
4) wnioskuje o nadanie upoważnień do przetwarzania danych osobowych pracownikom, zgodnie ze wzorem wniosku będącym załącznikiem Nr 5 do Polityki bezpieczeństwa,
5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Urzędzie.

§ 21. Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za realizację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

Rozdział III
WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

§ 22.1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej w postaci dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).

2. Wzór rejestru zbiorów danych osobowych oraz programów do przetwarzania tych danych prowadzonego przez ABI stanowi załącznik Nr 6 do Polityki bezpieczeństwa.

§ 23. Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Urzędzie wyróżnia się dwie kategorie danych:

1) **dane osobowe zwykłe** - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych.
2) **dane osobowe szczególnie chronione** – zgodnie z art.27 ust.1 ustawy o ochronie danych osobowych wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 24. Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, istnieje obowiązek zgłoszenia zbiorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a tejże ustawy.

Rozdział IV
UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

§ 25.1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:

1) jakie dane osobowe zawiera zbiór,
2) w jaki sposób zebrano dane,
3) w jakim celu i zakresie dane są przetwarzane,
4) w jakim zakresie oraz komu dane zostały udostępnione.

2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

3. ABI prowadzi wykaz udostępnień danych osobowych osobom, których dotyczą. Wzór wykazu stanowi załącznik Nr 7 do Polityki bezpieczeństwa.

§ 26.1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane,
7) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych,
9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1 - 5, nie częściej niż raz na 6 miesięcy.

§ 27.1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takiej wiadomości ma obowiązek o wystąpieniu osoby, której dane dotyczą, poinformować ABI.

§ 28.1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest kierownik jednostki lub pracownik posiadający wymagane prawem upoważnienie.

2. W przypadku udostępniania danych osobowych w celach innych niż wyłączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

3. Wzór wykazu udostępnień danych osobowych innym podmiotom, prowadzonego przez ABI, stanowi załącznik Nr 8 do Polityki bezpieczeństwa.

§ 29.1. Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez ADO z uwzględnieniem wymagań określonych w art.31, ust.1 tejże ustawy.

2. Administrator Bezpieczeństwa Informacji prowadzi wykaz podmiotów, którym powierzono przetwarzanie danych osobowych. Wzór w/w wykazu stanowi załącznik Nr 9 do Polityki bezpieczeństwa.

Rozdział V

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 30.1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki , winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

2. Sposób przepływu danych pomiędzy poszczególnymi systemami przedstawia załącznik Nr 10 do Polityki.

3. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się w relacji jednostka organizacyjna - zakład ubezpieczeń społecznych, urząd skarbowy, banki, urząd wojewódzki, urząd marszałkowski i inne jednostki administracji samorządowej i rządowej.

Rozdział VI
OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 31. Zabezpieczenie organizacyjne:

1) wyznaczono Administratora Bezpieczeństwa Informacji (ABI),
2) została opracowana i wdrożona polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
3) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,
4) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
5) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
6) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy,
7) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
8) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.

§ 32. Zabezpieczenie fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektronicznej:

1) dane osobowe, które są przedmiotem przetwarzania zgodnie z przepisami ustawy o ochronie danych osobowych, gromadzone i przechowywane są w serwerach i w postaci tradycyjnej,

2) za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe oraz sprzętu informatycznego przetwarzającego dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz kierownicy komórek organizacyjnych,
3) środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego,
4) pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż. (zasady przydziału kluczy do pomieszczeń, biurek i szaf regulują odrębne przepisy wewnętrzne Urzędu),
5) wzór wykazu pomieszczeń, w których przetwarzane są dane osobowe, a także stosowanego zabezpieczenia fizycznego stanowi załącznik Nr 11 do Polityki bezpieczeństwa,
6) w pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe,
7) dokumenty i wydruki oraz nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych,
8) użytkownicy zobowiązani są do stosowania „polityki czystego biurka", polegającą na zabezpieczeniu dokumentów w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia,
9) użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie,
10) użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

§ 33. Zabezpieczenie infrastruktury informatycznej i telekomunikacyjnej obejmuje zabezpieczenie serwera, sprzętu komputerowego i systemów informatycznych. Szczegółowa lista zabezpieczeń zawarta jest w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" (§ 3 Instrukcji).

§ 34. Zabezpieczenie programów i aplikacji przetwarzających dane osobowe opisane zostało w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" (§ 4 Instrukcji).

Rozdział VII

ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU

§ 35. Użytkownicy systemu zobowiązani są stosować odpowiednie środki bezpieczeństwa w pomieszczeniach, w których zainstalowano sprzęt systemu informatycznego by nie spowodować jego uszkodzenia.

§ 36.1. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

2. Hasło użytkownika podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł. W przypadku, gdy użytkownik zapomni swoje hasło, może on odnowić hasło w porozumieniu z Administratorem Systemu Informatycznego.

Rozdział VIII

INCYDENTY ZAGRAŻAJĄCE BEZPIECZEŃSTWU DANYCH OSOBOWYCH

§ 37. Każda osoba upoważniona do przetwarzania danych osobowych oraz zobowiązana do poufności danych osobowych w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązana jest poinformować o tym fakcie Administratora Bezpieczeństwa Informacji oraz swojego bezpośredniego przełożonego.

§ 38. Sposób postępowania z zagrożeniami określa „Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w Urzędzie Miejskim Gminy Łobżenica"

Rozdział IX

KONTROLA WEWNĘTRZNA STANU OCHRONY DANYCH OSOBOWYCH

§ 39. Za przeprowadzenie kontroli (sprawdzenia) ochrony danych osobowych w Urzędzie odpowiada Administrator Bezpieczeństwa Informacji.

§ 40. Kontroli podlegają: zbiory, systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami U.O.D.O.

§ 41.1. ABI przygotowuje plan sprawdzeń (kwartalny lub roczny) uwzględniając zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania. W okresie 5 lat należy dokonać kontroli wszystkich zbiorów i systemów Administratora Danych. Wzór planu sprawdzeń przedstawia załącznik Nr 12 do Polityki bezpieczeństwa.

2. ABI ma obowiązek przedstawienia ADO planu sprawdzeń najpóźniej na 2 tygodnie przed dniem rozpoczęcia okresu objętego planem.

3. ABI prowadzi sprawdzenia zgodnie z planem lub może wszcząć sprawdzenia doraźne na skutek podejrzenia lub naruszenia ochrony danych osobowych.

4. ABI zobowiązany jest do powiadomienia ADO oraz kierowników kontrolowanych komórek organizacyjnych o kontroli w terminie co najmniej 7 dni przed jej przeprowadzeniem.

5. ABI może dokumentować przebieg kontroli w postaci danych i wydruków z kontrolowanych systemów (programów), sporządzanie notatek z czynności, w szczególności z zebranych ustnych wyjaśnień, prowadzonych oględzin oraz sporządzanie kopii dokumentów, printscreenów, logów systemowych, zapisów konfiguracji technicznych środków zabezpieczeń systemów.

§ 42.1. Po dokonanej kontroli, ABI przygotowuje i przekazuje do ADO sprawozdanie ze sprawdzenia. W przypadku sprawdzenia planowego, sprawozdanie powinno być przekazane ADO nie później niż w terminie 30 dni od zakończenia sprawdzenia, natomiast w przypadku sprawdzenia doraźnego, sprawozdanie powinno być dostarczone do ADO niezwłocznie po zakończeniu sprawdzenia.

2. Wzór sprawozdania ze sprawdzenia stanowi załącznik Nr 13 do Polityki bezpieczeństwa.

Rozdział X
NADZÓR NAD DOKUMENTACJĄ PRZETWARZANIA DANYCH

§ 43. Administrator Bezpieczeństwa Informacji sprawując nadzór dokonuje weryfikacji:

1) opracowania i kompletności „Polityki bezpieczeństwa" oraz „Instrukcji zarządzania systemem informatycznym",
2) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa,
3) stanu faktycznego w zakresie przetwarzania danych osobowych,
4) zgodności ze stanem faktycznym przewidzianych w „Polityce bezpieczeństwa" oraz „Instrukcji zarządzania systemem informatycznym" środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych,

§ 44.1. Weryfikacja realizowana jest poprzez kontrole wewnętrzne (sprawdzenia) lub poza sprawdzeniami, na podstawie zgłoszeń osób wykonujących obowiązki określone w Polityce i Instrukcji oraz własnymi inicjatywami ABI.

2. W przypadku wykrycia podczas weryfikacji nieprawidłowości ABI zawiadamia ADO o nieopracowaniu lub brakach w dokumentacji oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu (np. projekty aktualizacji dokumentacji).

3. Jeśli nieprawidłowości wykryte podczas przeprowadzenia weryfikacji dotyczą konkretnych osób, ABI instruuje osoby o prawidłowych procedurach działania, poucza osoby naruszające zasady ODO lub zawiadamia administratora danych, wskazując osobę odpowiedzialną za naruszenie zasad oraz jego zakres.

§ 45.1. Administrator Bezpieczeństwa Informacji może zorganizować roczne spotkanie podsumowujące stan ochrony danych osobowych, na którym dokonywana jest ocena funkcjonowania systemu ochrony danych osobowych oraz planowane są działania związane z poprawą stanu ochrony danych osobowych. Uczestnikami spotkania są: ABI oraz wybrane osoby odpowiedzialne za stan ochrony danych osobowych w Urzędzie.

2. ABI dokumentuje roczne podsumowanie stanu ochrony danych osobowych i przekazuje "Roczny raport stanu Systemu Ochrony Danych Osobowych w Urzędzie Miejskim Gminy w Łobżenicy" Administratorowi Danych Osobowych. Wzór raportu przedstawia załącznik Nr 14 do Polityki bezpieczeństwa.

Rozdział IX
PRZEPISY KOŃCOWE

§ 46. Za naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

- *Art.49.1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których nie jest uprawniony , podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2;*
  2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
- *Art. 51. 1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*
  2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- *Art. 52. Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- *Art. 53. Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- *Art. 54. Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- *Art. 52. Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- *Art. 53. Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
- *Art. 54. Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

§ 47. W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

(Dz. U. z 2015 r. poz. 2135 z późn. zm.) 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. z 2004 r. Nr 100, poz. 1024).

OŚWIADCZENIE

Imię i nazwisko	
Stanowisko służbowe	
Nazwa komórki organizacyjnej	

Zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. , poz. 1182, 1662) zobowiązuję się do ochrony przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, danych osobowych przetwarzanych w Urzędzie oraz do zachowania ich w tajemnicy w czasie trwania jak i po ustaniu zatrudnienia.

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w Urzędzie dotyczących ochrony danych osobowych – w szczególności określonych w „Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim Gminy Łobżenica " oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim Gminy w Łobżenicy".

Oświadczam, że zapoznałem(am) się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r., poz. 2135 z późn. zm.), w tym z zasadami odpowiedzialności karnej określonymi w wyżej wymienionej ustawie.

....

(imię, nazwisko i podpis osoby przyjmującej oświadczenie)

(podpis osoby składającej oświadczenie)

Łobżenica, dnia .....

Załącznik Nr 2 do Polityki Bezpieczeństwa - Upoważnienie

UPOWAŻNIENIE NR .....

DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana .....

o numerze PESEL .....

zatrudnioną/-ego na stanowisku .....

w Urzędzie Miejskim Gminy w Łobżenicy.

do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:

Lp.	NAZWA ZBIORU DANYCH OSOBOWYCH

2. Identyfikator/Login: .....

3. Okres trwania upoważnienia: od dnia ..... do dnia .....

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

ADMINISTRATOR
DANYCH OSOBOWYCH

Łobżenica, dnia .....

Załącznik Nr 3 do Polityki Bezpieczeństwa – Ewidencja osób upoważnionych

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Numer upoważnienia	*Nazwisko i Imię*	*Komórka organizacyjna/Stanowisko*	*Identyfikator użytkownika systemu informatycznego*	*Data nadania upoważnienia*	*Data ustania upoważnienia*
ROK					
/	*Zakres upoważnienia*				
/	*Zakres upoważnienia*				
/	*Zakres upoważnienia*				
/	*Zakres upoważnienia*				

Załącznik Nr 4 do Polityki Bezpieczeństwa – Wniosek - zgłoszenie / zmiana zbioru danych osobowych

Łobżenica,.....

WNIOSEK
zgłoszenie / zmiana* zbioru danych osobowych

.....
(kierownik komórki organizacyjnej / pracownik na samodzielnym stanowisku pracy)

wnioskuję

o rejestrację nowego zbioru danych osobowych / zmianę zbioru danych osobowych*:

1. Nazwa zbioru danych osobowych .....
   .....
2. Podstawa prawna upoważniająca do prowadzenia zbioru danych osobowych .....
   .....
   .....
3. Cel przetwarzania danych .....
   .....
4. Opis kategorii osób, których dane dotyczą .....
   .....
5. Zakres przetwarzania danych .....
   .....
   .....
   .....
   .....
6. Sposób zbierania danych do zbioru .....
   .....
7. Sposób udostępniania danych .....
   .....
8. Informacja o odbiorcach, lub kategoriach odbiorców, którym dane mogą być przekazywane
   .....
9. Informacja dotycząca ewentualnego przekazania danych do państwa trzeciego .....
   .....
10. Nazwa systemu, w którym są przetwarzane dane osobowe .....
    .....
11. Osoby upoważnione do przetwarzania zbioru danych osobowych .....
    .....

.....
(data i podpis Kierownika komórki organizacyjnej / pracownika na samodzielnym stanowisku pracy)

* niepotrzebne skreślić

Załącznik Nr 5 do Polityki Bezpieczeństwa – Wniosek o wydanie upoważnienia do przetwarzania danych osobowych

Łobżenica,.....

WNIOSEK
o wydanie upoważnienia do przetwarzania danych osobowych

wnioskuję

o wydanie upoważnienia/ cofnięcie upoważnienia z dnia .....

Pani /Panu* .....

zatrudnionej/emu w .....

na stanowisku .....

do przetwarzania danych osobowych wynikających z zakresu obowiązków pracowniczych z powodu:

a) podjęcia pracy na stanowisku .....
b) zmiany stanowiska .....
c) zmiany zakresu obowiązków pracowniczych .....
d) utworzenia nowego zbioru danych osobowych .....
.....
e) naruszenia zasad i sposobu przetwarzania danych osobowych .....
.....

1. Nazwa zbioru danych osobowych: .....
.....
2. Rodzaj uprawnień: Z - pełne prawa do zarządzania bazą danych, P- prawo do przeglądania*,
.....
3. Sposób i miejsce przetwarzania danych osobowych .....
.....

.....
(data i podpis Kierownika komórki organizacyjnej / pracownika na samodzielnym stanowisku pracy)

* niepotrzebne skreślić

REJESTR ZBIORÓW DANYCH OSOBOWYCH

Nazwa zbioru danych osobowych / Data rejestracji i aktualizacji zbioru	Oznaczenie ADO	Przedstawiciel ADO	Podmiot, któremu powierzono przetwarzanie danych	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Opis kategorii osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze	Sposób zbierania danych do zbioru	Sposób udostępniania danych ze zbioru	Oznaczenie odbiorców danych	Informacja dotycząca przekazania danych do państwa trzeciego	Nazwa systemu, w którym są przetwarzane dane osobowe	Wydział / biuro / Osoby upoważnione

Załącznik Nr 7 do Polityki Bezpieczeństwa – Wykaz udostępnień danych osobowych osobom, których dotyczą

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH OSOBOM KTÓRYCH DOTYCZĄ

Lp.	Imię i nazwisko osoby, której dane są udostępniane	Data udostępnienia	Rodzaj zbioru danych osobowych	Sposób udostępnienia *(np. papierowy wydruk danych)*

Załącznik Nr 8 do Polityki Bezpieczeństwa – Wykaz udostępnień danych osobowych innym podmiotom

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH INNYM PODMIOTOM

Lp.	Imię i nazwisko lub nazwa zbioru danych osobowych	Data udostępnienia	Nazwa podmiotu, któremu udostępniono dane osobowe	Cel udostępnienia	Zakres udostępnionych danych	Sposób udostępnienia *(np. papierowy wydruk danych, forma elektroniczna)*

Załącznik Nr 9 do Polityki Bezpieczeństwa – Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych

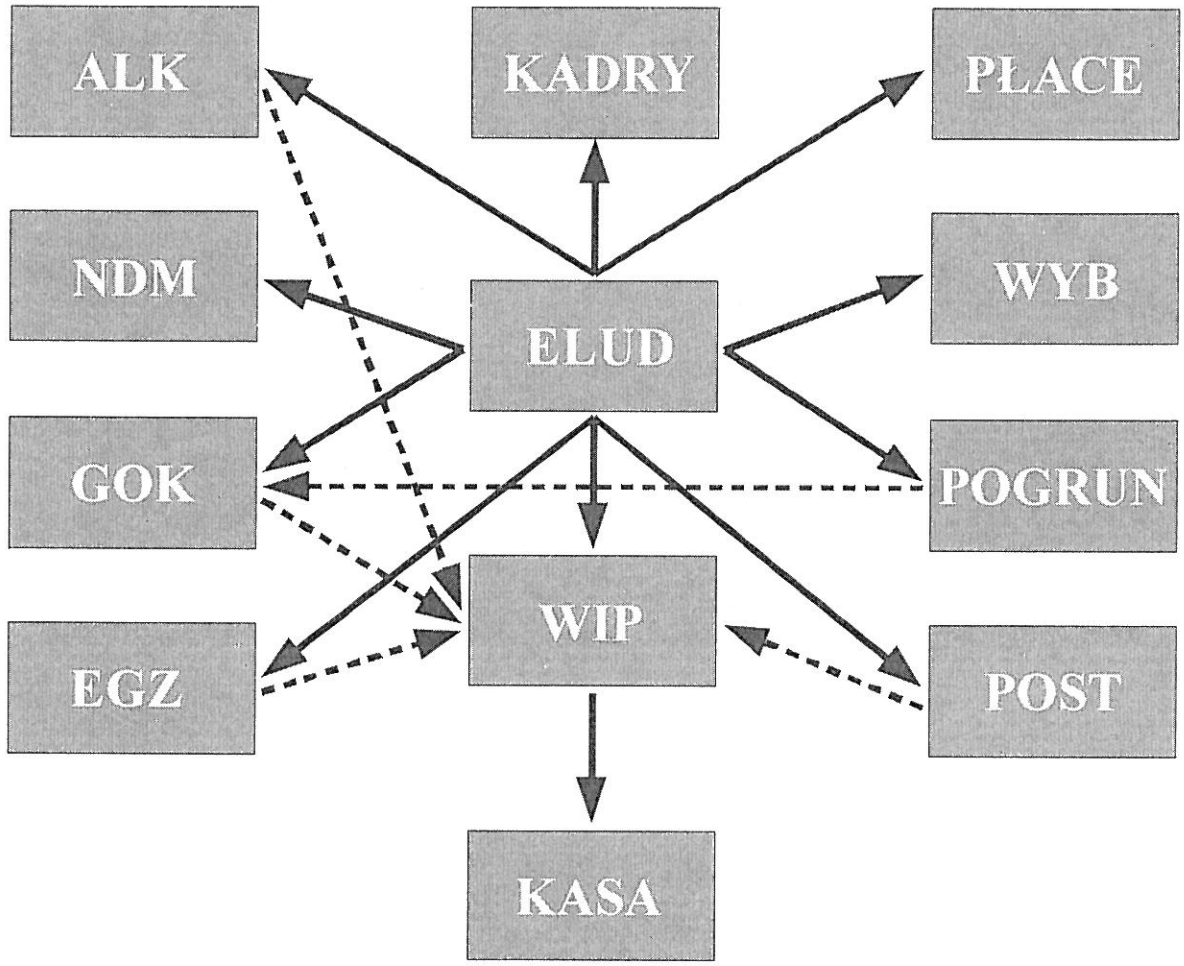
WYKAZ PODMIOTÓW, KTÓRYM POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH

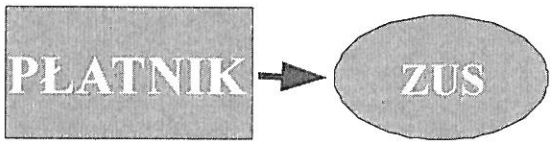
Lp.	Nazwa podmiotu, któremu powierzono dane osobowe	Numer umowy i data powierzenia	Nazwa zbioru danych osobowych	Cel udostępnienia	Zakres udostępnionych danych

Załącznik Nr 10 do Polityki Bezpieczeństwa – Sposób przepływu danych pomiędzy poszczególnymi systemami

PRZYKŁAD

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI





Załącznik Nr 11 do Polityki Bezpieczeństwa – Wykaz pomieszczeń, w których przetwarzane są dane osobowe

WYKAZ POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

Lp.	Lokalizacja - adres	Precyzyjne określenie pomieszczenia	Wydział/Osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia *

* KD – kontrola dostępu, A – alarm, K – kraty w oknach, DK –drzwi zamykane na klucz , KL – klimatyzacja, SP – sygnalizacja PPOŻ. GAS – gaśnice. SF - sejf, SMK- szafa metalowa zamykana na klucz, SDK- szafa zamykana na klucz

Załącznik Nr 12 do Polityki Bezpieczeństwa – Plan sprawdzeń

PLAN SPRAWDZEŃ	**Sporządził**	ABI
	Data:	
	Strona:	/

Plan sprawdzeń na okres	**... . ... . 20.... – ... . 20.... r.**
Numer i termin sprawdzenia	**Zakres sprawdzeń (kontroli)**
Nr ...../20..... ... . 20.... r.	**Sprawdzenie zgodności przetwarzania danych osobowych w zbiorze .....** 1. Przesłanek legalności przetwarzania danych osobowych zwykłych i wrażliwych 2. Merytorycznej poprawności danych i ich adekwatności do celu przetwarzania 3. Wykonania obowiązku informacyjnego (art. 24, art. 25, art. 33) 4. Zgłoszenia zbioru do rejestracji 5. Przekazywania danych do państwa trzeciego 6. Powierzenia przetwarzania danych 7. Udostępniania danych 8. Zabezpieczeń organizacyjnych, fizycznych, infrastruktury informatycznej i telekomunikacyjnej oraz programów i aplikacji
Nr ...../20..... ... . 20.... r.	**Sprawdzenie zgodności przetwarzania danych osobowych w zbiorze .....** 1. Przesłanek legalności przetwarzania danych osobowych zwykłych i wrażliwych 2. Merytorycznej poprawności danych i ich adekwatności do celu przetwarzania 3. Wykonania obowiązku informacyjnego (art. 24, art. 25, art. 33) 4. Zgłoszenia zbioru do rejestracji 5. Przekazywania danych do państwa trzeciego 6. Powierzenia przetwarzania danych 7. Udostępniania danych 8. Zabezpieczeń organizacyjnych, fizycznych, infrastruktury informatycznej i telekomunikacyjnej oraz programów i aplikacji

SPORZĄDZIŁ:

.....
(podpis ABI)

ZATWIERDZIŁ:

.....
(data, podpis ADO)

Załącznik Nr 13 do Polityki Bezpieczeństwa – Sprawozdanie ze sprawdzenia

SPRAWOZDANIE ZE SPRAWDZENIA **Nr ...../20.....**	**Sporządził**	ABI
	Data:	
	Strona:	/

Miejsce sprawdzenia:	**Termin wykonania sprawdzenia:** ... ... .20... r.
Nazwa administratora: Burmistrz Łobżenicy	**Przedmiot i zakres sprawdzenia:** .....
Podstawa sprawdzenia: ☐ - *sprawdzenie planowe,* ☐ - *sprawdzenie doraźne,* ☐ - *sprawdzenie specjalne*	

Wykaz czynności podjętych przez ABI w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach
1.
2.
3.

Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz Polityką bezpieczeństwa i Instrukcją zarządzania systemem informatycznym
1.
2.
3.

Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych, Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem
1.
2.
3.

KONTROLOWANI:

.....
.....
.....
.....
(data, podpisy kontrolowanych)

KONTROLER:

.....
(data, podpis ABI)

Załączniki:

1. Wydruki .....
2. .....

Załącznik Nr 14 do Polityki Bezpieczeństwa – Roczny raport stanu
Systemu Ochrony Danych Osobowych w Urzędzie Miejskim Gminy w Łobzenicy

Sprawozdanie – roczny raport stanu Systemu Ochrony Danych Osobowych w Urzędzie Miejskim Gminy Łobżenica za rok	**Sporządził**	ABI
	Data:	
	Strona:	/

Uczestnicy przeglądu rocznego:	**Termin przeprowadzenia przeglądu rocznego:**

Zagadnienia omawiane na przeglądzie:	**Komentarze / uwagi:**

Podsumowanie realizacji zadań z poprzedniego przeglądu *(zrealizowanych i w trakcie realizacji)*	
Omówienie wyników przeprowadzonych sprawdzeń w minionym roku	
Omówienie zarejestrowanych incydentów oraz ilości i powodów ich wystąpienia w minionym roku	
Proponowane zadania do realizacji	

SPORZĄDZIŁ: **ZATWIERDZIŁ:**

....

(podpis ABI) *(data, podpis ADO)*