

**POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
W STAROSTWIE POWIATOWYM W ŁOSICACH**

**Rozdział 1
Informacje ogólne**

§ 1

Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Starostwie Powiatowym w Łosicach odnosi się do danych osobowych przetwarzanych:

- 1) w zbiorach danych tradycyjnych, w szczególności w aktach prowadzonych spraw, rejestrach, wykazach i w innych zbiorach ewidencyjnych;
- 2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

§ 2

Ilekroć w niniejszym dokumencie jest mowa o:

- 1) Starostwo – w tym dokumencie jest rozumiane, jako Starostwo Powiatowe w Łosicach, z siedzibą w Łosice 08-200, ul. Narutowicza 6.
- 2) Administratorze Danych – należy przez to rozumieć Starostę Powiatu Łosickiego
- 3) Administratorze Bezpieczeństwa Informacji (ABI) – należy przez to rozumieć osobę wyznaczoną przez Starostę do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
- 4) Administratorze Systemu Informatycznego (ASI) – należy przez to rozumieć osobę wyznaczoną przez Starostę, odpowiedzialną za funkcjonowanie systemu informatycznego Starostwa oraz stosowanie technicznych i organizacyjnych środków ochrony;
- 5) użytkownika systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym starostwa, której nadano identyfikator i przyznano hasło, użytkownikiem może być pracownik Starostwa Powiatowego, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej lub osoba odbywająca staż, praktykę uczniowską studencką w Starostwie;
- 6) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Starostwa wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;

§ 3

Polityka bezpieczeństwa przetwarzania danych osobowych określa:

- 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- 4) sposób przepływu danych pomiędzy poszczególnymi systemami;

- 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 4

1. Do przetwarzania danych przechowywanych w systemie tradycyjnym i informatycznym mają dostęp jedynie upoważnieni pracownicy Starostwa oraz inne upoważnione osoby zajmujące się obsługą systemu. Wszyscy pracownicy zobowiązani są do zachowania danych w tajemnicy.
2. Dane patentów Starostwa Powiatowego są chronione zgodnie z polskim prawem oraz procedurami dotyczącymi bezpieczeństwa i poufności przetwarzanych danych obowiązującymi w Starostwie Powiatowym w Łosicach. Systemy tradycyjne i informatyczne, gdzie przechowywane są dane klientów Starostwa są chronione odpowiednimi środkami technicznymi i organizacyjnymi. Opracowane procedury określają obowiązki użytkownika oraz zasady korzystania z systemów. Każdy użytkownik systemu zobowiązany jest zapamiętać swoją nazwę użytkownika oraz hasło i nie udostępniać go innym osobom. Użytkownicy systemu powinni pamiętać o wylogowaniu się po zakończeniu korzystania z systemów informatycznych.

§ 5

1. Za bezpieczeństwo danych osobowych przetwarzanych w systemie tradycyjnym i informatycznym odpowiada Starosta Powiatu Łosickiego.
2. Administrator Danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Administrator Danych nadzoruje przestrzeganie zasad ochrony, prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych i prowadzi ewidencję osób upoważnionych do ich przetwarzania lub wyznacza inną osobę tj. Administratora Bezpieczeństwa Informacji do wykonywania tych czynności w zastępstwie. Druk powierzenia obowiązków Administratorowi Bezpieczeństwa Informacji stanowi **załącznik Nr 1**.
4. Administrator Danych wyznacza osobę odpowiedzialną za funkcjonowanie systemu informatycznego Starostwa oraz stosowanie technicznych i organizacyjnych środków ochrony, w tym: administrowanie systemami informatycznymi – instalowanie, aktualizowanie i zabezpieczanie systemów, przydzielanie haseł użytkownikom, przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego w którym przetwarzane są dane osobowe, ochronę antywirusową i wykonywanie kopii zapasowych - Administratora Systemu Informatycznego. Druk powierzenia obowiązków Administratorowi Systemu Informatycznego stanowi **załącznik Nr 2**.

Rozdział 2

Obszar przetwarzanych danych osobowych

§ 6

Obszar przetwarzania danych osobowych stanowią pomieszczenia Starostwa Powiatowego w Łosicach, ul. Narutowicza 6.

Rozdział 3

Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym i tradycyjnie

§ 7

Wykaz zbiorów danych osobowych przetwarzanych tradycyjnie i w systemie informatycznym ze wskazaniem programów zastosowanych do przetwarzania tych danych i miejscem przetwarzania określa **załącznik Nr 3**.

Rozdział 4

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

§ 8

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi określa **załącznik Nr 4**.

Rozdział 5

Sposób przepływu danych pomiędzy poszczególnymi systemami

§ 9

Dane z systemu „Płatnik” przesyłane są do ZUS w formie przekazu elektronicznego, w którym dane podpisane są certyfikatem kwalifikowanym.

Rozdział 6

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

§ 10

1. W Starostwie ze względu na połączenie z siecią publiczną stosuje się środki bezpieczeństwa określone dla wysokiego poziomu bezpieczeństwa. Bezpieczeństwo na poziomie wysokim zapewnia się poprzez ochronę fizyczną, sprzętową, ochronę w ramach oprogramowania systemowego i użytkowego - kontrolę dostępu do urządzeń systemu lub sieci komputerowej, ochronę kryptograficzną oraz środki organizacyjne. Zastosowane zabezpieczenia gwarantują:

- poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom
- integralność danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zamienione lub zniszczone w sposób nieautoryzowany
- rozliczalność – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
- integralność systemu – rozumie się przez to nienaruszalność systemu, niemożność jakiegokolwiek manipulacji,

2. Środki ochrony fizycznej:

- 1) pomieszczenia Starostwa Powiatowego 10-13 i od 15-25 wyposażone są w szyby antywłamaniowe, w pozostałych pomieszczeniach: 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 44, 46, 47, 48 w których przetwarzane są dane osobowe zabezpieczone elektronicznym system antywłamaniowym z całodobowym monitoringiem sygnału alarmu. Budynek Starostwa Powiatowego jest dozorowany całą dobę przez pracowników ochrony.
- 2) zbiory danych osobowych i urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zamykanych na klucze, które po zakończeniu urzędowania przekazywane są na portiernię Starostwa.
- 3) przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych;
- 4) użytkownik ma obowiązek zamykania systemu, programu po zakończeniu pracy, stanowisko komputerowe nie może pozostawać bez kontroli pracującego na nim użytkownika;
- 5) pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich;
- 6) monitory ekranowe są usytuowane w sposób uniemożliwiający odczyt danych przez osoby postronne;
- 7) obowiązkiem osoby użytkującej komputer przenośny zawierający dane osobowe jest zachowanie szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza pomieszczeniami tworzącymi obszar, w którym przetwarzane są dane osobowe, a także należy dążyć do powszechnego stosowania ochrony kryptograficznej w takich przypadkach;
- 8) kopie zapasowe przechowywane są w szafie metalowej w pomieszczeniu nr 31. Do dostępu do kopii zapasowych uprawnieni są: Administrator Danych, Administrator Bezpieczeństwa Informacji i Administrator Systemu Informatycznego;
- 9) zbiory danych przetwarzane tradycyjnie (ręcznie) po godzinach pracy przechowywane powinny być w szafkach zamkniętych na zamki, w przypadku przetwarzania takich danych w pomieszczeniu, w którym przebywać mogą osoby nieupoważnione do przetwarzania takich danych (np. interesanci albo inni pracownicy) należy przetwarzanie przeprowadzić w taki sposób, aby osoby nieupoważnione nie miały wglądu do tych danych.
- 10) w archiwum zakładowym drzwi wejściowe są antywłamaniowe z atestem, stalowe, zamykane są na podwójny zamek oraz zaplombowane.
- 11) w serwerowniach Starostwa zastosowane są drzwi antywłamaniowe z atestem, stalowe, z podwójnymi zamkami.

3. Środki sprzętowe, informatyczne i telekomunikacyjne:

- 1) zastosowano niszcarki dokumentów papierowych oraz nośników CD/DVD aby nośniki danych przeznaczone do wyrzucenia mogły być uprzednio zniszczone w sposób uniemożliwiający ich odczytanie, tzn. według normy DIN 66399 niszczenie nośników odbywa się co najmniej zgodnie z 3 stopniem tajności danych;
- 2) urządzenia sieciowe wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, dedykowanego dla sprzętu komputerowego.
- 3) sieć lokalna Starostwa Powiatowego chroniona jest przed zagrożeniami z sieci Internet poprzez zastosowanie zabezpieczeń na dwóch płaszczyznach:
 - a) zabezpieczenie połączenia z siecią Internet:
 - urządzenie typu firewall z uruchomioną usługą filtra stron www filtruje wchodzący i wychodzący ruch sieciowy na styku sieci LAN i Internet,
 - urządzenie typu IPS z dostępem do aktualnych sygnatur ataków - moduł sprzętowy urządzenia firewall - wykrywa niepożądany ruch w sieci i pomaga chronić ją przed włamaniami;

b) zabezpieczenie sieci LAN: w celu zwiększenia bezpieczeństwa sieć LAN została logicznie podzielona na sieci VLAN.

4. Środki ochrony w ramach oprogramowania systemu:

- 1) Dostęp do stacji roboczych oraz dostęp do programów służących do przetwarzania danych osobowych jest chroniony przez nazwę użytkownika i hasło. Każdy użytkownik ma inny identyfikator i przypisane mu uprawnienia do wykonywania operacji na danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Stosowane są systemowe mechanizmy kontrolujące składnię i czas życia haseł oraz ograniczające liczbę błędnych prób logowania.
- 2) system informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu;
- 3) w systemach operacyjnych zastosowano mechanizm wymuszający okresową zmianę haseł dostępu;
- 4) stosowane systemy operacyjne posiadają rozbudowane mechanizmy nadawania uprawnień i praw dostępu.
- 5) na wszystkich stacjach roboczych zainstalowano oprogramowanie antywirusowe z prawie codziennie aktualizowaną bazą wykrywanych wirusów, sprawdzające w trybie rzeczywistym wszystkie przychodzące i wychodzące pliki.
- 6) kopie bezpieczeństwa zbiorów danych osobowych wykonywane są codziennie automatycznie na dyskach komputera oraz raz w miesiącu po skompresowaniu programem do archiwizacji kopia miesięczna nagrywana jest na nośnik optyczny CD-R lub DVD-R. Kopie bezpieczeństwa są kopiami pełnymi. Za systematyczne przygotowywanie kopii bezpieczeństwa zbiorów danych osobowych i prowadzenie rejestru wykonanych miesięcznych kopii bezpieczeństwa odpowiada Administrator Systemów Informatycznych.
- 7) systemy operacyjne z rodziny Windows serwerów i komputerów rejestrują zdarzenia związane z logowaniem użytkowników w dzienniku zdarzeń.
- 8) dopuszcza się używanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania zadań ustawowych i posiadających ważną licencję użytkownika. Tylko Administrator Systemu Informatycznego jest uprawniony do instalowania i usuwania oprogramowania na stacjach roboczych użytkowników.
- 9) na dyskach lokalnych stacji roboczych nie mogą być gromadzone pliki nie związane z wykonanymi obowiązkami służbowymi. Zabronione jest wykorzystywanie poczty elektronicznej do celów innych niż służbowe. Nie należy korzystać z Internetu w celach innych niż służbowe. Zabronione jest korzystanie z systemów/aplikacji Starostwa, w których przetwarzane są dane osobowe, w celach innych niż służbowe.
- 10) zastosowano wygaszanie ekranu z opcją wymuszającą wprowadzenie hasła po wznowieniu w przypadku nieaktywności użytkownika trwającej 10 minut.

5. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

- 1) dla każdego użytkownika systemu jest ustalony odrębny identyfikator;
- 2) zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

6. Środki ochrony w ramach systemu użytkowego:

- 1) ekrany monitorów stanowisk dostępu do danych osobowych są automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika;
- 2) komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

7. Środki organizacyjne:

- 1) Administrator Danych wydaje imienne upoważnienia dla pracowników upoważnionych do przetwarzania danych osobowych w systemach informatycznych i zbiorach danych, według wzoru określonego w **załączniku Nr 5**;
- 2) Administrator Systemów Informatycznych przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnych upoważnień Administratora Danych określających zakres uprawnień pracownika.
- 3) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych w Starostwie według wzoru określonego w **załączniku Nr 6**;
- 4) osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem do tych danych :
 - zapoznawane z obowiązującymi przepisami o ochronie danych osobowych, w tym: ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.), rozporządzeniem 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. Nr 100, poz. 1024)
 - zapoznanie z polityką bezpieczeństwa przetwarzania danych osobowych i instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Łosicach podpisują oświadczenie, które stanowi **załącznik Nr 7**;
- 5) osoby upoważnione do przetwarzania danych osobowych obowiązane są do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczenia - zarówno w czasie zatrudnienia jak i po jego ustaniu.
- 6) sprzęt przekazywany do naprawy poza siedzibę Starostwa wcześniej pozbawiany jest nośników informacji zawierających dane osobowe.
- 7) przebywanie osób trzecich w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko pod ścisłą kontrolą osoby upoważnionej do przetwarzania danych osobowych.
- 8) przebywanie osób upoważnionych do przetwarzania danych osobowych w obszarze przetwarzania danych osobowych poza godzinami pracy jest dopuszczalne jedynie za zgodą Administratora Danych.
- 9) pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
- 10) w przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
- 11) zabronione jest wynoszenie nośników danych (dysków twardych, kart pamięci, pamięci USB, nośników optycznych, dyskietek) oraz urządzeń z tymi nośnikami, zawierających dane osobowe poza obszar przetwarzania danych osobowych, chyba że jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
- 12) nośniki i urządzenia zawierające dane osobowe można wynosić poza obszar przetwarzania danych wyłącznie za zgodą Administratora Danych, po uprzednim zaszyfrowaniu danych znajdujących się na tych nośnikach przez Administratora Systemów Informatycznych.
- 13) osoby użytkujące komputery przenośne zobowiązane są do zachowania szczególnej ostrożności podczas ich transportu, przechowywania i używania poza obszarem przetwarzania danych, w tym stosowania środków ochrony kryptograficznej.

Załącznik Nr 1
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Starostwie Powiatowym w Łosicach

Łosice, dnia

Wyznaczenie Administratora Bezpieczeństwa Informacji

1. Na podstawie art. 36 ust. 3 ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) z dniem r. **wyznaczam**

Pana/Panią

zam. legitymującą się
dowodem osobistym nr.....wydanym przez

na Administratora Bezpieczeństwa Informacji.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za bezpieczeństwo danych osobowych w zbiorach danych papierowych i w systemie informatycznym Starostwa, w tym w szczególności za nadzorowanie przestrzegania przez pracowników Starostwa w Łosicach zasad ochrony danych osobowych, nadzorowanie obiegu oraz przechowywania bieżących dokumentów zawierających dane osobowe oraz dokumentów zgromadzonych w archiwum, przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń i informowanie o tym Administratora Danych.

Tracą uprawnienia Administratora Bezpieczeństwa Informacji osoby wcześniej wyznaczone do pełnienia tych obowiązków.

.....
(podpis Administratora Bezpieczeństwa
Informacji)

.....
(podpis Starosty Powiatu Łosickiego)

Załącznik Nr 2
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Starostwie Powiatowym w Łosicach

Łosice, dnia

Wyznaczenie Administratora Systemu Informatycznego

1. Na podstawie art. 36 ust. 3 ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) z dniem r. **wyznaczam**
Pana/Panią
zam. legitymującą się dowodem osobistym
nr.....wydanym przez
na Administratora Systemu Informatycznego.
2. Administrator Systemu Informatycznego jest odpowiedzialny za funkcjonowanie systemów informatycznych oraz stosowanie technicznych i organizacyjnych środków ochrony, w tym: administrowanie systemami informatycznymi – instalowanie, aktualizowanie i zabezpieczanie systemów, przydzielanie identyfikatorów i haseł użytkownikom, przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego w którym przetwarzane są dane osobowe, ochronę antywirusową i wykonywanie kopii zapasowych.
3. Tracą uprawnienia Administratora Systemu Informatycznego osoby wcześniej wyznaczonej do pełnienia tych obowiązków.

.....
(podpis Administratora Bezpieczeństwa
Informatycznego)

.....
(podpis Starosty Powiatu Łosickiego)

Załącznik Nr 3
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Starostwie Powiatowym w Łosicach

Wykaz zbiorów danych osobowych przetwarzanych tradycyjnie i w systemie informatycznym ze wskazaniem programów zastosowanych do przetwarzania tych danych:

| Lp. | Referaty i samodzielne stanowiska | Nazwa zbioru danych osobowych | Sposób przetwarzania | |
|-----|---|--|----------------------|---|
| | | | Tradycyjny | W systemie Informatycznym podlegający zgłoszeniu do GODO (nazwa programu) |
| 1. | Referat Geodezji, Katastru i Nieruchomości | Opłaty za dzierżawy i użytkowanie wieczyste: <ul style="list-style-type: none"> ▪ ewidencja mienia gminy, powiatu lub Skarbu Państwa | X | MIENIE |
| | | Ewidencja gruntów i budynków: <ul style="list-style-type: none"> ▪ system ewidencji gruntów budynków i lokali wraz z kartoteką podatkową ▪ system grafiki komputerowej ▪ rejestr cen i wartości nieruchomości | X | EWOPIS EWMAPA REJCEN |
| | | Zgłoszenie robót geodezyjnych <ul style="list-style-type: none"> ▪ system ewidencji i zarządzania dokumentami w ośrodkach dokumentacji geodezyjnej i kartograficznej ▪ bank poziomych i wysokościowych osnów geodezyjnych | X | OŚRODEK BANK OSNÓW |
| | | Uzgodnienie danych projektowych: <ul style="list-style-type: none"> ▪ system ewidencji i zarządzania dokumentami w ośrodkach dokumentacji geodezyjnej i kartograficznej ▪ system grafiki komputerowej | X | OŚRODEK EWMAPA |
| 2. | Samodzielne stanowisko ds. obsługi Rady Powiatu | Centralny zbiór danych, z użyciem co najmniej jednego urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internet) | X | |
| | | Oświadczenia majątkowe Radnych Powiatu | X | |

| Lp. | Referaty i samodzielne stanowiska | Nazwa zbioru danych osobowych | Sposób przetwarzania | |
|-----|---|--|----------------------|---|
| | | | Tradycyjny | W systemie Informatycznym podlegający zgłoszeniu do GODO (nazwa programu) |
| 3. | Powiatowy Rzecznik Konsumentów | Rejestr w systemie komputerowym udzielonych porad prawnych konsumentom i interesantom w danym roku | X | |
| 4. | Referat Finansowy | Dane finansowo-księgowe | X | QNT Qwant |
| | | Dane przetwarzane w związku z zatrudnieniem, świadczeniem usług na podstawie umów cywilnoprawnych | X | Qwark, Płatnik |
| 5. | Referat Komunikacji | Dane przetwarzane w związku z wydawaniem kart parkingowych | X | |
| | | Akta pojazdów | X | |
| | | Akta kierowców i osób bez uprawnień | X | |
| 6. | Samodzielne stanowisko ds. kadr i organizacji | Dane zgromadzone w zbiorach danych osobowych | X | |
| | | Rejestr skarg i wniosków | X | |
| 7. | Samodzielne stanowisko ds. obronnych, obrony cywilnej i zarządzania kryzysowego | Dane teleadresowe Powiatowego Zespołu Zarządzania Kryzysowego Starosty Łosickiego | X | |
| 8. | Referat Architektury i Budownictwa | Rejestr wniosków o pozwolenie na budowę | X | |
| 9. | Referat Ochrony Środowiska, Rolnictwa i Leśnictwa | Rejestr: wydawanych kart wędkarskich; zaświadczeń rejestrowanego sprzętu pływackiego; strażników społecznych straży rybackiej. | X | |
| | | Wnioski: o wydanie świadectwa legalności pozyskania drzew w lesie; o przekazanie środków finansowych z ARiMR na wypłatę ekwiwalentów należnych właścicielom zalesionych gruntów rolnych i prowadzeniem upraw leśnych i wykazów tych upraw złożonych w ramach „PROW 2007-2013”. | X | |

Załącznik Nr 4
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Starostwie Powiatowym w Łosicach

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między zbiorami.

Dane przetwarzane w związku z zatrudnieniem, świadczeniem usług na podstawie umów cywilnoprawnych – Kadry (imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania, numer ewidencyjny PESEL, NIP, zawód, wykształcenie, seria i nr dowodu osobistego, numer telefonu oraz wynagrodzenie).

Dane finansowo-księgowe – Referat Finansowy (imię i nazwisko, adres, telefon, NIP, PESEL, konto bankowe).

Rejestr w systemie komputerowym udzielonych porad prawnych konsumentom i interesantom w danym roku – Powiatowy Rzecznik Konsumentów (imię i nazwisko lub inne oznaczenie interesanta, adres).

Zbiory danych osobowych – Referat Ochrony Środowiska, Rolnictwa i Leśnictwa (imię i nazwisko, adres zamieszkania, nr i seria dowodu osobistego).

Rejestr danych osobowych – Samodzielne stanowisko ds. obsługi Rady Powiatu (nazwisko i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, miejsce pracy, zawód, wykształcenie, numer telefonu, Numer Identyfikacji Podatkowej).

Rejestr danych osobowych – Referat Geodezji, Katastru i Nieruchomości (imię i nazwisko, adres zamieszkania).

Dane przetwarzane w związku z wydawaniem kart parkingowych, akta pojazdów, akta kierowców i osób bez uprawnień – Referat Komunikacji (imię i nazwisko, adres zamieszkania, nr dowodu, nr PESEL, data i miejsce urodzenia, dane dotyczące stanu zdrowia, telefon, adres e-mail).

Rejestr wniosków o pozwolenie na budowę – Referat Architektury i Budownictwa (imię i nazwisko, adres zamieszkania).

Dane teleadresowe Powiatowego Zespołu Zarządzania Kryzysowego Starosty Łosickiego – Samodzielne stanowisko ds. obronnych, obrony cywilnej i zarządzania kryzysowego (funkcja w zespole, służba, stanowisko, adres zamieszkania, telefon domowy, komórkowy, adres e-mail).

Rejestr skarg i wniosków, dane zgromadzone w zbiorach danych osobowych (imię i nazwisko, adres zamieszkania lub pobytu).

UPOWAŻNIENIE Nr/.....
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.), **upoważniam**
Pana/Panią

.....
(imię nazwisko)

.....
(stanowisko służbowe)

do przetwarzania następujących danych osobowych:

a)w zbiorach tradycyjnych:.....

.....
.....

(zbiór danych i zakres upoważnienia do jego przetwarzania)

b) w systemie informatycznym:

.....
.....
.....

(zbiór danych i zakres upoważnienia do jego przetwarzania)

.....
(data i podpis pracownika)

.....
(data i podpis Administratora Danych)

Załącznik Nr 6
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Starostwie Powiatowym w Łosicach

**EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH
OSOBOWYCH W STAROSTWIE POWIATOWYM W ŁOSICACH**

| Numer upoważnienia | nazwisko i imię osoby upoważnionej | Stanowisko służbowe | Zakres upoważnienia (zawartość zbioru danych) | Data nadania upoważnienia | Data ustania upoważnienia | Uwagi |
|--------------------|------------------------------------|---------------------|---|---------------------------|---------------------------|-------|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Łosice, dnia

.....
imię i nazwisko pracownika

OŚWIADCZENIE

Oświadczam, że zapoznałam/em się z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024) oraz zarządzeniem Nr 24/2012 Starosty Powiatu Łosickiego z dnia 26.10.2012r. w sprawie realizacji ustawy o ochronie danych osobowych i zobowiązuję się do przestrzegania zasad opisanych w:

- Polityce bezpieczeństwa przetwarzania danych osobowych
- Instrukcji zarządzania systemem informatycznym.

.....
czytelny podpis pracownika