Załącznik Nr 1
do Zarządzenia Nr 30/2009
Starosty Ząbkowickiego
z dnia 9.07.2009 r.

„Polityka bezpieczeństwa"
przetwarzania danych osobowych
w Starostwie Powiatowym w Ząbkowicach Śląskich

Opracował: Administrator Bezpieczeństwa Informacji

Ząbkowice Śląskie 2009 r.

SPIS TREŚCI:

ZAŁĄCZNIKI:

Załącznik nr 1. Wykaz zbiorów danych osobowych wraz nazwą systemu służącego do ich przetwarzania oraz ich strukturą

Załącznik nr 2. Wykaz obszarów, w których przetwarzane są dane osobowe

Załącznik nr 3. Wzór upoważnienia do pobierania kluczy i dostępu do pomieszczenia serwerowni

Załącznik nr 4. Wzór wniosku o wydanie upoważnienia do przetwarzania danych osobowych

Załącznik nr 5. Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 6. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 7. Wzór oświadczenia o zapoznaniu się z dokumentacją dotyczącą ochrony danych osobowych

Załącznik nr 8. Wzór ewidencji osób, które zostały zapoznane z dokumentacją dotyczącą ochrony danych osobowych

Załącznik nr 9. Wzór zgłoszenia z naruszenia bezpieczeństwa systemu informatycznego

Załącznik nr 10. Wzór raportu ze zgłoszenia naruszenia bezpieczeństwa systemu informatycznego

Załącznik nr 11. Wzór wniosku o udostępnienie danych ze zbioru danych osobowych

Załącznik nr 12. Wzór ewidencji udostępnienia danych osobowych

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa przetwarzania danych osobowych w sposób tradycyjny oraz w systemach informatycznych w Starostwie Powiatowym w Ząbkowicach Śląskich. Opisane reguły określają granice dopuszczalnego zachowania wszystkich pracowników biorących udział w przetwarzaniu danych osobowych w urzędzie.

Potrzeba jego opracowania wynika z § 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

<u>Polityka bezpieczeństwa obowiązuje wszystkich pracowników Starostwa Powiatowego w Ząbkowicach Śląskich.</u>

Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznym Urzędu.

1. Administrator Danych Osobowych, którym jest Starosta Ząbkowicki, wyznacza Administratora Bezpieczeństwa Informacji oraz zastępcę Administratora Bezpieczeństwa Informacji.
2. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   2) podejmowania stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,
   3) niezwłocznego informowania Administratora Danych Osobowych (Starosty) lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,

4) nadzoru i kontroli zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
5) fizycznego zabezpieczenia danych osobowych oraz obiektów, w których są gromadzone i przetwarzane.

3. W przypadku nieobecności Administratora Bezpieczeństwa Informacji powyższe zadania realizuje jego zastępca. Zastępca ze wszystkich podjętych działań składa Administratorowi Bezpieczeństwa Informacji relację w formie pisemnej notatki.

Polityka bezpieczeństwa danych osobowych została opracowana na podstawie następujących aktów prawnych:

1) ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
2) 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).

Definicje

- Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- Administrator Danych Osobowych - zadania administratora danych osobowych wykonuje Starosta Ząbkowicki.
- Administrator Bezpieczeństwa Informacji - osoba wyznaczona przez Administratora Danych Osobowych nadzorującą całokształt zagadnień związanych z ochroną danych osobowych
- Administrator Systemu Informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych.
- System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

- Bezpieczeństwo systemu informatycznego - wdrożenie przez Administratora Danych Osobowych środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
- Przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
- Osoba upoważniona - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych na wniosek Administratora Bezpieczeństwa Informacji i dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu (ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji).
- Użytkownik systemu - osoba posiadająca uprawnienia umożliwiające dostęp do systemu informatycznego, w którym są przetwarzane dane osobowe.
- Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
- Rozporządzenie - rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Rozdział 1
OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:
   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu; ciągłość pracy systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, obniżenie sprawności i wydajności sprzętu i oprogramowania związane z jego eksploatacją) – mogą prowadzić do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu lub nastąpić naruszenie poufności danych.

3) zagrożenia zamierzone – świadome i celowe działania powodujące naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
   - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
   - nieuprawniony dostęp do systemu z jego wnętrza (naruszenie zabezpieczeń),
   - nieuprawnione przekazanie danych,
   - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

2. Naruszenie lub podejrzenie naruszenia zabezpieczeń systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:
   1) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,
   2) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   3) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
   4) pojawienia się odpowiedniego komunikatu alarmowego,
   5) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
   6) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
   7) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,
   8) ujawnienia nieautoryzowanych kont dostępu do systemu,
   9) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.
   - niezabezpieczone pomieszczenia ze szczególnym uwzględnieniem pomieszczenia serwerowni,
   - nienadzorowane, otwarte szafy, biurka, regały,
   - niezabezpieczone urządzenia i nośniki do archiwizacji,
   - pozostawianie danych w nieodpowiednich miejscach – biurka, półki na dokumenty itp.

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem Danych Osobowych gromadzonych i przetwarzanych w sposób tradycyjny i w systemach informatycznych Urzędu jest Starosta Ząbkowicki (wykaz zbiorów danych osobowych przetwarzanych w Urzędzie wraz z nazwą systemu służącego do ich przetwarzania oraz ich strukturą stanowi załącznik nr 1 do niniejszego dokumentu).
2. Tworzenie nowego bądź modyfikacja struktury lub zakresu danych istniejącego zbioru podlega obowiązkowi zgłoszenia Administratorowi Danych Osobowych. Obowiązek spoczywa na osobie tworzącej lub modyfikującej zbiór danych osobowych.
3. Administrator Danych Osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych przetwarzanych w sposób tradycyjny oraz w systemach informatycznych Urzędu, a w szczególności:
   1) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiega przed pobraniem danych przez osobę nieuprawnioną,
   3) zapobiega zmianie, utracie, uszkodzeniu lub zniszczeniu danych,
   4) zapewnia przetwarzanie danych zgodnie z obowiązującymi przepisami prawa.
4. Techniczną ochronę danych i ich przetwarzania realizuje się poprzez:
   1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach,
   2) zabezpieczenie pomieszczeń, o których mowa w pkt. 1, przed nieuprawnionym dostępem:
      - klucze do pomieszczeń, w których następuje przetwarzanie danych osobowych wydawane są tylko osobom upoważnionym do przetwarzania danych w tych pomieszczeniach,
      - pomieszczenia, w których odbywa się przetwarzanie danych osobowych znajdują się pod ścisłym nadzorem pracujących w nim osób upoważnionych do przetwarzania danych,
   3) zabezpieczenie dostępu do komputerów, na których jest prowadzone przetwarzanie danych przez wprowadzenie systemu logowania zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego, określonymi w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,
   4) systematyczne wykonywanie kopi bezpieczeństwa danych na nośnikach zewnętrznych przechowywanych w sejfach,
   5) zastosowanie zasilaczy UPS do zasilania awaryjnego serwerów, urządzeń dostępowych oraz wszystkich komputerów,
   6) aktywowanie na wszystkich stacjach roboczych ochrony antywirusowej,

7) stosowanie zapory ogniowej (firewall) na ruterach dostępowych zabezpieczającej sieci przed atakiem z zewnątrz i filtrującej dostęp do sieci WAN poprzez blokowanie niektórych usług,
8) umieszczenie większości urządzeń znajdujących się w serwerowniach w szafach serwerowych i sieciowych oraz wyposażenie pomieszczeń serwerowni w klimatyzację zapewniającą właściwą temperaturę i wilgotność,
9) wyposażenie pomieszczeń w zamykane na klucz i dające gwarancję bezpieczeństwa dokumentacji drzwi, szafy, biurka, itp.

5. Organizacyjne środki ochrony danych osobowych i ich przetwarzania obejmują:
   1) zapoznanie każdej osoby upoważnionej z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu,
   2) przeszkolenie użytkowników systemu w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych oraz zabezpieczeniem pomieszczeń i budynków,
   3) szczególne zabezpieczenie pomieszczenia serwerowni, do którego dostęp posiadają jedynie osoby upoważnione na piśmie przez Administratora Danych Osobowych (Starostę), wzór upoważnienia stanowi załącznik nr 3 do niniejszego dokumentu,
   4) dopuszczenie do przetwarzania danych osobowych jedynie osób posiadających upoważnienie oraz prowadzenie ewidencji tych osób.
6. Do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych Osobowych w toku następującej procedury:
   1) bezpośredni przełożony pracownika kieruje do Administratora Bezpieczeństwa Informacji wniosek o wydanie upoważnienia do przetwarzania danych osobowych określając:
      - dane użytkownika
      - zbiór danych osobowych
      - zakres przetwarzanych danych osobowych,

      (wzór wniosku stanowi załącznik nr 4 do niniejszego dokumentu)
   2) Administrator Bezpieczeństwa Informacji przedkłada Administratorowi Danych Osobowych (Staroście) do akceptacji wniosek oraz upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik nr 5)

3) po zaakceptowaniu przez Starostę wniosku i wystawieniu upoważnienia
   - Administrator Bezpieczeństwa Informacji zapoznaje nowego użytkownika z Polityką bezpieczeństwa, Instrukcją zarządzania systemami informatycznymi, Ustawą i Rozporządzeniem oraz wprowadza użytkownika do ewidencji osób zapoznanych z dokumentacją (wzór stanowi załącznik nr 8) oraz do ewidencji osób upoważnionych do przetwarzania danych osobowych (wzór stanowi załącznik nr 6),
   - zapoznanie się z powyższymi regulacjami pracownik potwierdza Administratorowi Bezpieczeństwa Informacji własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 7 do niniejszego dokumentu

7. Modyfikacja lub odebranie pracownikowi upoważnienia do przetwarzania danych osobowych następuje na pisemny wniosek przełożonego pracownika i podlega analogicznej procedurze jak przy jego nadawaniu.
8. Przepływ danych pomiędzy systemami informatycznymi służącymi do przetwarzania danych osobowych odbywa się w poszczególnych budynkach Urzędu z wykorzystaniem wewnętrznej zamkniętej sieci LAN. Wymiana danych pomiędzy zamkniętymi sieciami LAN (pomiędzy budynkami) realizowana jest za pomocą łącza stałego VDSL2 wykorzystującego parę przewodów miedzianych łączących budynki.
9. Wykaz obszarów, w których przetwarzane są dane osobowe stanowi załącznik nr 2 do niniejszego dokumentu.
10. Niezależnie od niniejszych ustaleń mają zastosowanie wszelkie inne regulaminy i instrukcje dotyczące bezpieczeństwa.

Rozdział 3
KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator Bezpieczeństwa Informacji sprawuje w imieniu Administratora Danych Osobowych nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikający z ustawy o ochronie danych osobowych, zasad ustanowionych w niniejszym dokumencie oraz instrukcji zarządzania systemami informatycznymi.
2. Każdy pracownik Starostwa Powiatowego w Ząbkowicach Śląskich jest zobowiązany poddać się kontroli wynikającej z ochrony danych osobowych prowadzanej przez Administratora Bezpieczeństwa Informacji oraz udostępnić niezbędne informacje mające wpływ na bezpieczeństwo danych.

3. Na podstawie kontroli oraz zgłoszeń naruszenia bezpieczeństwa danych osobowych, Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie, które przedstawia Staroście.

Rozdział 4
POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,

   oraz innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, kradzież itp.)

   każda osoba zatrudniona w Starostwie jest zobowiązana do niezwłocznego powiadomienia o fakcie naruszenia bezpieczeństwa ochrony danych osobowych bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji.
2. Po stwierdzeniu naruszenia opisanego w ust. 1 należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
   4) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
   5) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub jego zastępcy,
   7) niezwłocznie po przybyciu Administratora Bezpieczeństwa Informacji wypełnić zgłoszenie faktu naruszenia ochrony danych osobowych (wzór zgłoszenia stanowi załącznik nr 9).

3. Po przybyciu na miejsce naruszenia lub ujawnienia danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowej pracy Urzędu,
   2) może zażądać dokładnej relacji na piśmie z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3) w razie potrzeby powiadamia o zaistniałym naruszeniu Administratora Danych Osobowych,
   4) jeżeli zachodzi taka potrzeba zleca usuniecie występujących naruszeń Administratorowi Systemów Informatycznych oraz powiadamia odpowiednie instytucje.
4. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 10.
5. Raport, o którym mowa w ust. 4, Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych Osobowych (Staroście).
6. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Starostę.
7. Analiza, o której mowa w pkt. 6, powinna zawierać wszechstronną ocenę zaistniałego naruszenia oraz wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5

ZASADY UDOSTĘPNIENIA DANYCH OSOBOWYCH.

1. Dane osobowe gromadzone i przetwarzane w Urzędzie mogą być udostępniane wyłącznie osobom uprawnionym na podstawie wniosku o udostępnienie danych osobowych zaakceptowanego przez Administratora Danych Osobowych (wzór wniosku stanowi załącznik nr 11 do niniejszego dokumentu) lub realizującym zadania ustawowe.
2. Bez względu na formę udostępniania danych należy zachować ich poufność i integralność. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną ani inną uniemożliwiającą ustalenie tożsamości osoby uzyskującej dostęp do danych.
3. Każde udostępnienie danych osobowych należy odnotować w ewidencji, która powinna zawierać, co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych. Wzór ewidencji stanowi załącznik nr 12 do niniejszego dokumentu.

4. Obowiązek prowadzenia ewidencji spoczywa na osobie odpowiedzialnej za eksploatację zbioru danych i udostępniającej dane osobowe lub innej wyznaczonej przez bezpośredniego przełożonego.
5. Ewidencję należy udostępnić do wglądu na każde żądanie Administratora Bezpieczeństwa Informacji.

Rozdział 6
POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
3. W kwestiach nieuregulowanych w niniejszym dokumencie a dotyczących bezpieczeństwa danych osobowych w Starostwie Powiatowym w Ząbkowicach Śląskich decyzje na wniosek zainteresowanego wydaje Administrator Danych Osobowych (Starosta).