Załącznik do Zarządzenia Nr 17 /2013

Wójta Gminy Wodzisław
z dnia 3 kwietnia 2013 r.

Polityka bezpieczeństwa
dotycząca przetwarzania danych osobowych
w Urzędzie Gminy w Wodzisławiu

Spis treści: str.

Rozdział I

Postanowienia ogólne.

§ 1

1. Polityka bezpieczeństwa dotycząca przetwarzania danych osobowych w Urzędzie Gminy w Wodzisławiu zwana dalej „Polityką", jest dokumentem, którego celem jest określenie podstawowych reguł dotyczących zapewnienia bezpieczeństwa w zakresie przetwarzania danych osobowych:
    1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
    2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
2. Urząd Gminy w Wodzisławiu , zwany dalej „Urzędem", realizując Politykę dokłada szczególnej staranności w celu zabezpieczenia bezpieczeństwa danych osobowych poprzez zapewnienie ich poufności, integralności i dostępności, w tym w szczególności aby dane te były:
    1) przetwarzane zgodnie z prawem,
    2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane przetwarzaniu niezgodnemu z tymi celami,
    3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakim są przetwarzane,
    4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
3. Urząd realizując Politykę dąży do systematycznego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Polityka obowiązuje wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w Urzędzie.
5. Polityka została opracowana na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwaną dalej „ustawą o ochronie danych osobowych", oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać

urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)

6. Polityka bezpieczeństwa podlega okresowej aktualizacji, która jest realizowana Sekretarza Gminy.

§ 2

Ilekroć w Polityce jest mowa o:

1) Administratorze Danych Osobowych – zwanym dalej Administratorem należy przez to rozumieć Wójta Gminy Wodzisław .
2) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
3) danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
4) danych osobowych wrażliwych – rozumie się przez to dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatach karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
5) zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
6) Urzędzie – rozumie się przez to Urząd Gminy w Wodzisławiu.
7) Instrukcji – rozumie się przez to Instrukcję zarządzania systemem informatycznym, która obowiązuje w Urzędzie Gminy w Wodzisławiu .
8) Administratorze Bezpieczeństwa Informacji, zwanym dalej ABI - należy przez to rozumieć osobę wyznaczoną przez Administratora i odpowiedzialną za nadzorowanie przestrzegania zasad ochrony przetwarzanych danych osobowych w Urzędzie Gminy, w tym w szczególności związanych z przeciwdziałaniem dostępowi do danych osobowych osób nieupoważnionych, zabraniu przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem oraz przetwarzaniem danych z naruszeniem ustawy o ochronie danych osobowych.
9) Administratorze Systemów Informatycznych, zwanym dalej ASI - należy przez to rozumieć osobę wyznaczoną przez Administratora, której cele działania jest nadzorowanie, kontrolowanie zasad bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.

10) użytkowniku - należy przez to rozumieć pracownika Urzędu, który posiada upoważnienie wydane przez Administratora lub osobę upoważnioną przez niego i dopuszczoną, w zakresie w nim wskazanym do przetwarzania danych osobowych w danej jednostce organizacyjnej urzędu.
11) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
12) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
13) osobie trzeciej – należy przez to rozumieć każdą osobę nieupoważnioną i przez to nieuprawnioną do dostępu do danych osobowych będących w posiadaniu Administratora. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez Administratora podejmująca czynności w zakresie przekraczającym ramy jego upoważnienia.
14) systemie informatycznym, zwanym dalej systemem – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
15) zabezpieczeniu systemu informatycznego – należy przez to rozumieć wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.
16) przetwarzaniu danych osobowych – należy przez to rozumieć wykonywanie jakichkolwiek operacji na danych osobowych, m.in. takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie,
17) usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
18) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom (osobom),
19) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
20) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu (użytkownika) mogą być przypisane w sposób jednoznaczny temu podmiotowi (użytkownikowi),
21) uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (użytkownika),
22) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby upoważnionej do przetwarzania danych,
    c) przedstawiciela podmiotu przetwarzającego dane osobowe mającego siedzibę lub miejsce zamieszkania w państwie trzecim,

d) podmiotu, któremu powierzono przetwarzanie danych osobowych w drodze umowy,
e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Rozdział II
Zasady przetwarzania danych osobowych

§ 3

1. Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy:
   1) osoba, której dane dotyczą, wyrazi zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
   2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
   3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
   4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
   5) jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
2. Każda z przesłanek wymienionych w ust. 1 jest autonomiczna i może stanowić samodzielną podstawę przetwarzania danych osobowych.
3. Zgoda osoby, której dane osobowe dotyczą jest oświadczeniem woli, którego treścią jest zgoda na przetwarzanie jego danych osobowych w określonym celu, w określonym zakresie, przez określonego administratora danych osobowych. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. W przypadku zgody na przetwarzanie danych osobowych wrażliwych zgoda musi być wyrażona na piśmie.

§ 4

1. W przypadku zbierania danych osobowych od osoby, której dane dotyczą należy zapewnić informację dla tej osoby o:
   1) nazwie i siedzibie administratora danych osobowych,
   2) celu zbierania danych, a w szczególności o znanych lub przewidywanych odbiorcach danych osobowych,
   3) prawie dostępu do treści swoich danych oraz ich poprawiania,
   4) dobrowolności lub obowiązku podania danych osobowych, a jeżeli taki obowiązek istnieje o jego podstawie prawnej.
2. Przepisu ust. 1 nie stosuje się, jeżeli:

1) przepis innej ustawy zezwala na przetwarzanie danych osobowych bez ujawniania faktycznego celu ich zbierania,
2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

Rozdział III

Zarządzanie zbiorami danych osobowych

§ 5

1. ASI prowadzi wykaz zbiorów danych osobowych zwany dalej wykazem zbiorów.
2. Każdy zbiór opisany jest w wykazie zbiorów przez nazwę, podstawę przetwarzania, zakres przetwarzanych danych osobowych, formę przetwarzania, nazwę aplikacji, nazwę jednostek organizacyjnych urzędu przetwarzających dane osobowe w zbiorze.
3. Zabrania się przetwarzania danych osobowych w zbiorach, które nie figurują w wykazie zbiorów.
4. Zabrania się przetwarzania danych osobowych w zbiorze, w stosunku do którego istnieje obowiązek zgłoszenia do rejestru GIODO przed dokonaniem tego zgłoszenia.
5. Zabrania się przetwarzania danych osobowych w zbiorach, zawierających dane osobowe wrażliwe przed dokonaniem rejestracji przez GIODO. Rejestracja takiego zbioru potwierdzona jest zaświadczeniem o zarejestrowaniu zbioru danych, które wydaje GIODO.
6. Zobowiązuje się pracowników i kierowników jednostek organizacyjnych do informowania ABI o planowaniu utworzenia zbioru danych osobowych.
7. Utworzenie nowego zbioru danych osobowych może być wynikiem:
    1) realizacji nowego celu,
    2) zidentyfikowania zbioru, który nie został wpisany do wykazu zbioru,
    3) przyjęcia zbioru danych osobowych w wyniku zawarcia umowy o powierzeniu przetwarzania.
8. Tworzenie nowego zbioru w systemie informatycznym może nastąpić tylko po uzgodnieniach i po akceptacji przez ABI.
9. Tworzenie nowego zbioru w formie dokumentu papierowego może nastąpić po akceptacji ABI.
10. W przypadku konieczności zarejestrowania nowego zbioru w rejestrze GIODO wniosek rejestracyjny na platformie e- giodo wypełnia ABI. ABI wypełnia wniosek od pkt 1 do pkt 16 w części dotyczącej środków ochrony fizycznej.
11. Wypełniony wniosek rejestracyjny na platformie e- giodo przesyłany jest przez ASI w postaci elektronicznej po uzupełnieniu go w zakresie dotyczącym opisu środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej oraz środków ochrony w ramach narzędzi programowych i baz danych. Kompletny wniosek przesyłany jest w postaci elektronicznej do ABI.
12. ABI po uzupełnieniu wniosku w zakresie środków organizacyjnych, sprawdzeniu czy wszystkie wymagane elementy wniosku są wypełnione przesyła go do GIODO.
13. Dokumenty związane z rejestracją zbioru danych przechowuje ASI.

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

§ 6

1. ASI przekazuje niezwłocznie do ABI informacje aktualizujące opis zbioru danych osobowych w wykazie zbiorów danych osobowych.
2. Aktualizacji zgłoszeń w rejestrze GIODO wymagają w szczególności następujące sytuacje:
   1) dokonanie zmian w warunkach technicznych związanych ze zgłoszonym zbiorem danych osobowych, wpływających na zmianę treści zgłoszenia,
   2) dokonanie zmian w warunkach organizacyjnych związanych ze zgłoszonym zbiorem danych osobowych, wpływających na zmianę treści zgłoszenia,
   3) zmiana podstaw prawnych lub celu przetwarzania danych osobowych ,
   4) zmiana zakresu przetwarzanych danych osobowych oraz zmiana kategorii osób, których dane dotyczą,
   5) zmiana odbiorców lub kategorii odbiorców, którym dane mogą być przekazywane,
   6) zmiana sposobu zbierania oraz udostępniania danych osobowych.
3. W przypadku konieczności aktualizacji zgłoszenia w rejestrze GIODO w związku z sytuacją określoną ust. 2 pkt 2- 6 potrzebę w tym zakresie zobowiązany jest zgłosić niezwłocznie ASI do ABI. Procedura aktualizacji zgłoszenia zbioru do GIODO odpowiada procedurze zgłoszenia zbioru do rejestracji opisanej w § 5.
4. W przypadku zmian środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej lub środków ochrony w ramach narzędzi programowych i baz danych potrzebę dokonania aktualizacji zgłoszenia zbioru do GIODO określa ASI. Jeśli konieczna jest aktualizacja zgłoszenia wówczas ASI wypełnia wniosek aktualizacyjny na platformie e-giodo i przesyła w postaci elektronicznej do ABI, który dokonuje aktualizacji w rejestrze GIODO.
5. Zabrania się dokonywania zmian warunków technicznych i organizacyjnych związanych z ochroną danych osobowych bez konsultacji z ABI.
6. Zabrania się dokonywania zmian w zbiorze przetwarzanych danych osobowych, w przypadku gdy zmiana dotyczy rozszerzenia zakresu przetwarzania danych osobowych o dane osobowe wrażliwe przed zgłoszeniem tej zmiany do GIODO.

§ 7

1. Działania związane z wyrejestrowaniem zbioru danych osobowych z rejestru GIODO podejmuje ABI .
2. Decyzja GIODO o wyrejestrowaniu zbioru danych jest podstawą wykreślenia zbioru z wykazu zbiorów.
3. W przypadku zbiorów danych, które nie są zarejestrowane przez GIODO, wykreślenie z wykazu zbiorów dokonuje ABI.

§ 8

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

Rozdział IV

Opis zdarzeń naruszających ochronę danych osobowych

§ 9

1. Naruszenie ochrony danych osobowych, może być spowodowane:
   1) niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, skutki powodzi, pożaru, itp.,
   2) niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu,
   3) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe lub osób odpowiedzialnych za ich ochronę.
2. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   1) przetwarzanie danych osobowych bez właściwego upoważnienia,
   2) przetwarzanie danych osobowych z naruszeniem zasad opisanych w § 3,
   3) przetwarzanie danych osobowych w zbiorach nieujętych w wykazie zbiorów,
   4) brak możliwości fizycznego dostępu do danych w wyniku np. zagubionego klucza do pomieszczenia, lub mebli biurowych, w których przechowywane są dokumenty, zniszczonej szafy z dokumentami, braku nośników informacji itp.,

5) brak dostępu do zawartości zbioru danych pomimo, że zbiór istnieje,
6) zmienioną w sposób nieuprawniony zawartość zbioru, niepoprawną treść, postać, datę, różnicę w danych itp.,
7) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia w którym jest przetwarzany,
8) zniszczenie lub próby zniszczenia w sposób nieautoryzowany danych ze zbioru lub danych systemowych,
9) zmianę lub utratę danych zapisanych na kopiach zapasowych lub zapisach archiwalnych,
10) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (dyskietki, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione,
11) próba nielegalnego logowania się do systemu lub włamania do systemu,
12) zmienione oprogramowanie systemu, stwierdzone przez użytkownika.

§ 10

Zakazuje się przekazywania danych osobowych przez łącza teleinformatyczne niezabezpieczone.

Rozdział V

Zasady postępowania w sytuacji naruszenia ochrony danych osobowych

§11

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz ABI lub osobę wskazaną przez ABI.
2. Użytkownik do momentu przybycia ABI lub osoby przez niego wskazanej powinien:
   1) zabezpieczyć dostęp do pomieszczenia lub urządzenia;
   2) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony;
   3) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony;
   4) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych.
3. Po przybyciu na miejsce osoby, o której mowa w ust. 2 realizuje ona czynności w kolejności:

1) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych;
2) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia;
3) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony;
4) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń;

4. ABI z przebiegu zdarzenia sporządza raport z naruszenia bezpieczeństwa przetwarzania danych osobowych, który przekazuje Administratorowi lub osobie przez niego upoważnionej.
5. Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowanie przetwarzania danych wyraża Administrator.
6. Dokonywanie zmian w miejscu naruszenia ochrony bez zgody ABI jest dopuszczalne tylko w wypadku konieczności ratowania osób, mienia albo zapobieżenia powstaniu innego niebezpieczeństwa.

Rozdział VI

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

§ 12

1. W Urzędzie obowiązujące zasady użytkowania systemów informatycznych służących do przetwarzania danych osobowych określa Instrukcja.
2. Instrukcja, o której mowa w ust. 1 jest opracowywana przez ASI i następnie zatwierdzana przez Administratora. ASI wdraża Instrukcję do użytku w Urzędzie.

§ 13

1. Dane osobowe w Urzędzie mogą być przetwarzane tylko przez osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Administratora. Upoważnienie określa zakres uprawnień do wykonywania operacji na danych osobowych.
2. W Urzędzie prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
3. Zadanie prowadzenia ewidencji, o której mowa w ust. 2 realizuje ASI . Ewidencja może być prowadzona w postaci elektronicznej.
4. Ewidencja o której mowa w ust. 2 powinna zawierać:
   1) numer porządkowy,
   2) imię i nazwisko użytkownika,

3) nazwę komórki organizacyjnej, w której jest zatrudniony,
4) datę nadania upoważnienia do przetwarzania danych,
5) zakres upoważnienia do przetwarzania danych osobowych,
6) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym,
7) datę ustania upoważnienia do przetwarzania danych osobowych,
8) nr i datę wydania zaświadczenia o odbyciu szkolenia w zakresie ochrony danych osobowych lub datę podpisania oświadczenia, o którym mowa w § 14 ust. 11.

5. Zmiana informacji wyszczególnionych w ewidencji podlega niezwłocznemu odnotowaniu.

§ 14

1. Upoważnienie do przetwarzania danych osobowych dla pracowników Urzędu wydawane jest, z zastrzeżeniem § 29, po złożeniu wniosku przez kierownika jednostki organizacyjnej lub jego przełożonego do ABI o udzielenie wskazanej osobie upoważnienia do przetwarzania danych osobowych. We wniosku określany jest zakres uprawnień do przetwarzania danych osobowych, który uwzględnia zakres realizowanych zadań.
2. Upoważnienie do przetwarzania danych osobowych dla osób nie będących pracownikami Urzędu następuje na wniosek właściwego merytorycznie kierownika jednostki organizacyjnej lub jego przełożonego, który składany jest do ABI. We wniosku określany jest zakres uprawnień do przetwarzania danych osobowych, który uwzględnia zakres realizowanych zadań.
3. Wzór wniosku o upoważnienie do przetwarzania danych osobowych zawiera załącznik nr 1 do Polityki.
4. Wzór upoważnienia do przetwarzania danych osobowych w Urzędzie zawiera załącznik nr 5 do Polityki.
5. Projekt upoważnienia opracowuje ABI . Administrator może upoważnić ABI do podpisywania upoważnień do przetwarzania danych osobowych.
6. Upoważnienie do przetwarzania danych osobowych jest rejestrowane przez ABI w ewidencji osób upoważnionych do przetwarzania danych osobowych.
7. Po wydaniu upoważnienia ABI pisemnie przekazuje o tym informację właściwemu kierownikowi jednostki organizacyjnej.
8. W przypadku upoważnienia do przetwarzania danych osobowych w systemie informatycznym informacja ta przekazywania jest również do ASI w celu zapewnienia zarejestrowania użytkownika w systemie. Procedura związana z rejestracją użytkownika w systemie informatycznym jest określona w Instrukcji.
9. W przypadku potrzeby zmiany zakresu uprawnień do przetwarzania danych osobowych konieczne jest ponowne złożenie wniosku. Upoważnienie o zmienionym brzmieniu rejestrowane jest w ewidencji osób upoważnionych do przetwarzania danych osobowych.

10. Upoważnienie wykonywane jest w trzech egzemplarzach, jeden otrzymuje osoba ubiegająca się o upoważnienie, pozostałe przechowywane są w komórce kadrowej oraz u ABI.
11. Upoważnienie dla osoby, o której mowa w ust. 2 wydawane jest po podpisaniu przez nią oświadczenia o zobowiązaniu się do zachowania w tajemnicy, także po ustaniu realizacji zadań, poznanych danych osobowych oraz informacji związanych z funkcjonowaniem systemu ochrony danych osobowych. Upoważnienie to jest ważne na czas realizacji zadań ustalonych z Administratorem.
12. Wzór oświadczenia, o którym mowa w ust. 11 zawiera załącznik nr 4 do Polityki.
13. Upoważnienia i oświadczenia, o którym mowa w ust. 11 wykonywane są w trzech egzemplarzach. Odpowiednio jeden egzemplarz otrzymuje upoważniona osoba, drugi właściwa merytorycznie jednostka organizacyjna, trzeci przechowywany jest u ABI.
14. Nadzór nad przestrzeganiem zasad ochrony danych osobowych przez osobę, o której mowa w ust. 2 realizuje właściwy merytorycznie kierownik jednostki organizacyjnej Urzędu.

§ 15

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

§ 16

1. Użytkownik traci aktualne upoważnienie do przetwarzania danych osobowych w sytuacjach:
   1) ustania zatrudnienia użytkownika u Administratora,
   2) zmiany zakresu obowiązków użytkownika,
   3) ustania wykonywania zadań przez osoby nie będące pracownikami Urzędu w związku z którymi otrzymały upoważnienia.
2. Przełożeni użytkowników zobowiązani są do niezwłocznego przekazywania informacji ABI w przypadku zaistnienia okoliczności powodujących utratę upoważnienia lub do ASI i ABI jeśli upoważnienie to dotyczy przetwarzania danych osobowych w systemie informatycznym.
3. Informację, o której mowa w ust.2 w przypadku osób nie będących pracownikami przekazuje kierownik jednostki organizacyjnej, o którym mowa w § 14 ust. 2.
4. Stanowisko ds.kadr i płac przekazuje informacje do ABI o ustaniu zatrudnienia pracownika w Urzędzie jak również o przeniesieniu pracownika do innej jednostki organizacyjnej Urzędu. Informację taką należy przekazać również w przypadku posiadanie wiedzy o planowaniu wcześniej wymienionych zdarzeń.
5. W przypadku, gdy upoważnienie dotyczy przetwarzania danych osobowych w systemie informatycznym wyrejestrowanie z systemu następuje zgodnie z Instrukcją .
6. Ustanie upoważnienia odnotowywane jest w ewidencji osób upoważnionych do przetwarzania danych osobowych.

§ 17

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

§ 18

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

§ 19

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

§ 20

1. Dane osobowe przetwarza się w budynkach, pomieszczeniach lub częściach pomieszczeń, tworzących obszar przetwarzania danych osobowych, który określany jest przez Administratora lub osobę przez niego upoważnioną.
2. Przebywanie osób trzecich w pomieszczeniach, w którym są przetwarzane dane osobowe jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
3. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe są zamykane na czas nieobecności użytkowników, uniemożliwiając do nich dostęp.
4. Zasady zabezpieczenia pomieszczeń i budynków po zakończeniu pracy określają właściwe instrukcje opracowywane przez jednostkę organizacyjną Urzędu odpowiedzialną za administrowanie jego obiektami w porozumieniu z kierownikami jednostek organizacyjnych użytkujących pomieszczenia w określonym budynku. Instrukcje podlegają uzgodnieniu z ABI a następnie zatwierdzane są przez Administratora Danych.
5. Instrukcje, o których mowa w ust. 5 określają zasady otwierania i zamykania budynków oraz pomieszczeń a także zasady ich sprzątania.

§ 21

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonanie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do przetwarzania danych.

§ 22

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

§ 23

1. Codzienną kontrolę bezpieczeństwa przetwarzania danych osobowych sprawują użytkownicy oraz ich przełożeni. Okresową kontrolę sprawują ASI oraz ABI.
2. Kierownik jednostki organizacyjnej Urzędu odpowiedzialny jest za prowadzenie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane. Okresowo powyższą kontrolę wykonuje ASI.
3. ABI opracowuje roczny plan kontroli w zakresie ochrony danych osobowych, który zatwierdza Administrator .
4. ASI opracowuje roczny plan kontroli w zakresie ochrony danych osobowych w systemach informatycznych urzędu, który zatwierdza Administrator.

§ 24

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu danych, w sposób uniemożliwiający ich odzyskanie,
   3) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.

2. W celu zapewnienie nieprzerwanej i bezpiecznej pracy systemów informatycznych prowadzone są okresowe przeglądy i konserwacje, które zapewnia AS. Zasady prowadzenia przeglądów i konserwacji urządzeń komputerowych, systemów informatycznych oraz zbiorów danych określa Instrukcja.
3. W celu zapewnienia ochrony serwerów przed utratą danych w wyniku awarii zasilania stosuje się zasilacze awaryjne UPS.
4. W celu zapewnienia ochrony przed utratą danych stosuje się zasilacze awaryjne UPS przy stacjach roboczych odpowiednio do potrzeb.

§ 25

1. Systemy informatyczne służące do przetwarzania danych osobowych muszą być wyposażone w mechanizmy kontroli dostępu do tych danych.

2. Środki stosowane do uwierzytelniania w systemie informatycznym oraz zarządzanie identyfikatorami i hasłami określa Instrukcja.
3. Hasło podlega szczególnej ochronie, zakazuje się użytkownikowi jego udostępnianiu innym osobom. Przełożeni, osoby dokonujące przeglądów i konserwacji jak i innych prac związanych z systemem informatycznym muszą posiadać upoważnienia oraz własne identyfikatory i hasła umożliwiające dostęp do systemów informatycznych.

§ 26

1. Użytkownicy systemów przetwarzających dane osobowe nie mogą instalować oraz uruchamiać żadnych aplikacji, które nie zostały wcześniej dopuszczone do użytkowania w Urzędzie.
2. W Urzędzie systemy, w których przetwarzane są dane osobowe wyposażone są w mechanizmy ochrony antywirusowej. Stosowanie tych mechanizmów oraz ich skuteczność kontroluje ASI.
3. W Urzędzie systemy posiadają zabezpieczenie przed działaniem oprogramowania mającego na celu uzyskanie nieuprawnionego dostępu do tych systemów. Za stosowanie tych zabezpieczeń odpowiada ASI.

§ 27

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

§ 28

ASI zapewnia aby system informatyczny, w którym przetwarzane są dane osobowe – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – dla każdej osoby, której dane są przetwarzane odnotowywał w sposób automatyczny po zatwierdzeniu przez użytkownika operacji wprowadzenia danych oraz umożliwiał sporządzenie i wydrukowanie raportu w powszechnie zrozumiałej formie zawierającej:

1) datę pierwszego wprowadzenia danych do systemu,
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jeden użytkownik,
3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
4) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,
5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

§ 29

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

§ 30

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

Rozdział VII

Przepisy końcowe

§ 31

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który stanowi załącznik nr 6 do Polityki prowadzi ASI.