KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Załącznik Nr 1
Do zarządzenia Nr 28/2015
Wójta Gminy Secemin
z dnia 27 kwietnia 2015 r.

Urząd Gminy Secemin

Polityka Bezpieczeństwa

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych

Projekt „e-Urząd – satysfakcja, komfort i wygoda dla Mieszkańców” współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

SPIS TREŚCI

I. WSTĘP

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych Urzędu Gminy Secemin (zwana dalej: „Polityką Bezpieczeństwa") określa zasady i tryb postępowania przy przetwarzaniu danych osobowych.

Polityka Bezpieczeństwa została opracowana zgodnie z wymogami określonymi w § 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 obowiązuje wszystkich pracowników Urzędu Gminy Secemin oraz dostawców, podmioty współpracujące na zasadzie umów, mające jakikolwiek kontakt z danymi osobowymi objętymi ochroną (np. osoby realizujące zadania na podstawie umów zlecenia lub o dzieło, stażystów, praktykantów, serwisantów).
Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. **poufność danych** - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. **integralność danych** - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. **integralność systemu** rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r. poz. 1182, z późn. zm.),
2. oraz aktami wykonawczymi wydanymi na podstawie ww, ustawy.

Użyte w Polityce Bezpieczeństwa określenia oznaczają:

1. **ustawa (u.o.d.o.)** - Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r. poz. 1182, z późn. zm.),
2. **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 (Dz. U. z 2004 r. Nr 100, poz. 1024),
3. **Administrator Danych Osobowych (ADO)** - Wójt Gminy Secemin, który decyduje o celach i środkach przetwarzania danych osobowych w Urzędzie Gminy Secemin oraz monitoruje wdrożone zabezpieczenia systemu informatycznego,

4. **Administrator Bezpieczeństwa Informacji (ABI)-** rozumie się przez to pracownika Urzędu Gminy wyznaczonego przez Administratora Danych Osobowych, nadzorującego przestrzeganie zasad, o których mowa w art. 36 ust. 1 u.o.d.o.
5. **Administrator Systemu Informatycznego** - osoba odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób nieupoważnionych do systemów oraz podejmowanie odpowiednich działań w przypadku stwierdzenia naruszeń w tych systemach,
6. **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
7. **osoba możliwa do zidentyfikowania** - każda osoba fizyczna, 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,
8. **zbiór danych osobowych** - posiadający strukturę zestaw danych o charakterze danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcyjnie,
9. **przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalenie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
10. **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych; za system informatyczny uważany jest również pojedynczy komputer wraz z oprogramowaniem, przy pomocy którego przetwarzane są dane osobowe,
11. **zabezpieczenie danych osobowych** - środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacja, ujawnieniem lub pozyskaniem danych osobowych lub ich utratą,
12. **Instrukcja** - Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

II. Określenie osób pełniących funkcje Administratora Danych Osobowych i Administratora Bezpieczeństwa Informacji oraz inne funkcje związane z zapewnieniem właściwej ochrony danych osobowych w Urzędzie Gminy Secemin.

1) Administrator Danych Osobowych

Funkcję **Administratora Danych Osobowych** pełni Wójt Gminy Secemin.

Do podstawowych obowiązków Administratora Danych Osobowych należy:

1. przetwarzanie danych osobowych zgodnie z prawem;
2. dopełnienie obowiązku zgłoszenia zbiorów danych osobowych do rejestracji GIODO, za wyjątkiem przypadków określonych w art. 43 ustawy. Obowiązkowi rejestracji zbiorów danych osobowych z wyjątkiem zbiorów zawierających dane wrażliwe nie podlega

administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi Ochrony Danych osobowych do rejestracji.

3. dopełnienie obowiązku informacyjnego ustanowionego w art. 24 ust. 1 oraz art. 25 ust. 1 u.o.d.o.;
4. dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą;
5. respektowanie prawa osób, których dane dotyczą;
6. stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
7. wydawanie i odbieranie upoważnień do przetwarzania danych;
8. prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych;
9. podejmowanie działań w przypadku wykrycia naruszeń w systemie bezpieczeństwa danych osobowych;
10. kontrolowanie, jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane;
11. udzielanie informacji o zakresie przetwarzanych danych osobowych;
12. spełnienie obowiązku uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane;
13. zapewnienie środków finansowych niezbędnych do ochrony danych osobowych.

2) POWOŁANIE, REJESTRACJA, ZMIANA I ODWOŁANIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI.

1. Administrator Danych Osobowych może powołać administratora bezpieczeństwa informacji (**Załącznik Nr 1**).,
2. Administratorem Bezpieczeństwa Informacji może być osoba, która:

   2.1) ma pełną zdolność do czynności prawnych oraz korzystania z pełni praw publicznych,

   2.2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,

   2.3) nie była karana za umyślne przestępstwo.

3. Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania.
4. Zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji powinno zawierać:

   4.1) oznaczenie administratora danych i adres jego siedziby lub zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;

   4.2) dane administratora bezpieczeństwa informacji:

      a) imię i nazwisko,

      b) numer PESEL lub, gdy ten numer nie został nadany, nazwę i numer dokumentu stwierdzającego tożsamość,

      c) adres do korespondencji, jeżeli jest inny niż adres o którym mowa w pkt.4.1),

4.3) datę powołania,

4.4) oświadczenie administratora danych o spełnieniu przez administratora bezpieczeństwa informacji warunków określonych w pkt 2.

5. Wzory zgłoszeń powołania, zmiany informacji objętych zgłoszeniem i odwołania administratora bezpieczeństwa informacji do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, określają załączniki do Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934).
6. Administrator danych jest obowiązany zgłosić Generalnemu Inspektorowi zmianę informacji objętych zgłoszeniem, o którym mowa w pkt 4), w terminie do 14 dni od dnia zmiany. Do zgłaszania zmian stosuje się odpowiednio przepisy o zgłoszeniu powołania administratora bezpieczeństwa informacji.
7. Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań określonych w pkt. II.3). Administrator Bezpieczeństwa Informacji.
8. Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki określone w pkt. 2.
9. Administrator Bezpieczeństwa Informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej Administratorem Danych.
10. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w pkt. II.3). Administrator Bezpieczeństwa Informacji, z wyłączeniem obowiązku sporządzenia sprawozdania, wykonuje administrator danych.

3) Administrator Bezpieczeństwa Informacji

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za:

1. prowadzenie dokumentacji dotyczącej bezpieczeństwa danych osobowych;
2. prowadzenie i nadzorowanie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych;
3. prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów o których mowa w art. 43 ust. 1,
4. opracowanie sprawozdania z sprawdzenia wykonywanego na wniosek Generalnego Inspektora u administratora danych, który go powołał. Zawartość sprawozdania określa art. 36c. u.o.d.o.;
5. prowadzenie ewidencji zbiorów danych osobowych przetwarzanych w Urzędzie Gminy;
6. prowadzenie wykazu obszarów przetwarzania danych osobowych w Urzędzie Gminy;
7. wydawanie i odbieranie upoważnień do przetwarzania danych;
8. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
9. sprawowanie nadzoru nad prawidłowym stosowaniem się do zasad i procedur określonych w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy Secemin;
10. sprawowanie nadzoru nad fizycznym zabezpieczeniem obszarów przetwarzania danych osobowych oraz kontrolę przebywających w nich osób;
11. sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;

12. sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;
13. sprawowanie nadzoru nad instalacjami i konfiguracjami oprogramowania systemowego, sieciowego oraz bazodanowego;
14. sprawowanie nadzoru nad profilaktyką antywirusową;
15. sprawowanie nadzoru w zakresie wykonywanych kopii zapasowych danych osobowych;
16. sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentacji zawierającej dane osobowe;
17. sprawowanie nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemach informatycznych Urzędu Gminy oraz kontrolę dostępu do danych;
18. identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone mogą być dane osobowe przetwarzane w Urzędzie Gminy;
19. monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych;
20. przeprowadzanie kontroli w zakresie ochrony danych osobowych;
21. określanie potrzeb w zakresie zabezpieczenia danych osobowych ;
22. aktualizacje jawnego rejestru zbiorów danych osobowych przetwarzanych przez Urząd Gminy;
23. podejmowanie odpowiednich działań w przypadkach naruszenia bezpieczeństwa danych osobowych;
24. prowadzenie rejestru incydentów i zdarzeń wskazujących na naruszenie bezpieczeństwa danych osobowych;
25. zatwierdzanie procedur bezpieczeństwa i standardów zabezpieczeń wnioskowanych i obowiązujących w Urzędzie Gminy;
26. dokonywanie modyfikacji i akceptacji proponowanych zmian, jak i okresowych kontroli polityk i procedur;
27. umożliwienie przeprowadzenia kontroli przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych;
28. sprawowanie nadzoru nad procesem przyznawania praw dostępu;
29. organizowanie szkoleń z zakresu ochrony danych osobowych;
30. opiniowanie zakupów nowych systemów informatycznych;
31. opiniowanie wzorów dokumentów i umów;
32. nadzorowanie Administratora Systemów Informatycznych;
33. nadzorowanie osób upoważnionych do przetwarzania danych osobowych;
34. prowadzenie metryczek zbiorów danych osobowych;
35. zapewnienie, aby dane osobowe prowadzone zbiorach były:

a) przetwarzane zgodnie z prawem,
b) zbierane dla oznaczonych i zgodnych z prawem celów,
c) merytorycznie poprawne i adekwatne w stosunku do celu w jakich są przetwarzane,
d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą;

36. przygotowywanie wniosków zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych osobowych;
37. prowadzenie aktualnego wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
38. zapewnienie poufności, integralności i rozliczalności danych osobowych;
39. określenie indywidualnych obowiązków i odpowiedzialności osób upoważnionych do przetwarzania danych osobowych;
40. sprawowanie nadzoru nad prawidłowym stosowaniem się do zasad i procedur określonych w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemami Informatycznymi;
41. zapewnienie szkoleń osobom, które będą dopuszczone do przetwarzania danych osobowych;

42. dopuszczanie do przetwarzania danych osobowych wyłącznie osób upoważnionych do przetwarzania danych osobowych;
43. sprawowanie nadzoru nad właściwym eksploatowaniem systemów informatycznych;
44. sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentacji zawierającej dane osobowe;

4) ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

Administrator Systemów Informatycznych odpowiedzialny jest za:

1. bieżący nadzór oraz zapewnienie ciągłości działania systemów informatycznych;
2. optymalizację wydajności systemów informatycznych;
3. zabezpieczenie systemów informatycznych;
4. zarządzanie konfiguracją systemów i urządzeń wchodzących w skład systemu informatycznego;
5. przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych w systemach informatycznych;
6. dokonywanie okresowej analizy ryzyka dla poszczególnych systemów informatycznych wykorzystywanych do przetwarzania danych osobowych;
7. prowadzenie dokumentacji systemowej opisującej działania związane z administracją systemów informatycznych, w których przetwarzane są dane osobowe;
8. przyznawanie na wniosek Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do systemów informatycznych;
9. współpracę z dostawcami aplikacji i sprzętu komputerowego w tym sieciowego i serwerowego;
10. wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń;
11. opracowywanie procedur dotyczących bezpieczeństwa i standardów zabezpieczeń w systemach informatycznych;
12. udostępnianie danych zgromadzonych w systemach informatycznych na wniosek Administratora Danych Osobowych oraz za zgodą Administratora Bezpieczeństwa Informacji;
13. bieżące wykonywanie kopii systemowych jak i kopii baz danych i aplikacji wykorzystywanych do przetwarzania danych osobowych;
14. świadczenie wsparcia technicznego w ramach oprogramowania oraz serwis sprzętu komputerowego wchodzącego w skład systemów informatycznych Urzędu Gminy;
15. diagnozowanie i usuwanie awarii sprzętu komputerowego oraz utrzymywanie kontaktu z firmami świadczącymi usługi pogwarancyjne sprzętu komputerowego;
16. prowadzenie dokumentacji dotyczącej opisu struktury zbiorów danych osobowych oraz udostępnianie jej Administratorowi Bezpieczeństwa Informacji;
17. prowadzenie dokumentacji dotyczącej opisu przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych oraz udostępnianie jej Administratorowi Bezpieczeństwa Informacji;
18. prowadzenie ewidencji sprzętu i oprogramowania służącego do przetwarzania danych osobowych;
19. umożliwienie przeprowadzenia kontroli przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych;
20. sprawowanie nadzoru nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji;

21. wykonywanie napraw oraz konserwacji systemów informatycznych a także likwidację urządzeń komputerowych oraz elektronicznych nośników zawierających dane osobowe;
22. sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;
23. sprawowanie nadzoru nad profilaktyką antywirusową;
24. zapewnienie szkoleń Pracowników Urzędu w zakresie prawidłowego korzystania z aplikacji i urządzeń wchodzących w skład systemów informatycznych służących do przetwarzania danych osobowych;
25. opiniowanie zakupów dotyczących urządzeń sieciowych i serwerowych;
26. opiniowanie zakupów dotyczących oprogramowania sieciowego, serwerowego oraz narzędziowego;

III. ZASADY DOPUSZCZANIA PRACOWNIKÓW URZĘDU GMINY SECEMIN DO PRZETWARZANIA DANYCH OSOBOWYCH, OBOWIĄZKI NAŁOŻONE NA PRACOWNIKÓW DOPUSZCZONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ REJESTRACJI/AKTUALIZACJI ZBIORU DANYCH DO GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH.

1) DOPUSZCZENIE PRACOWNIKÓW DO PRZETWARZANIA DANYCH OSOBOWYCH.

1. Do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby posiadające imienne upoważnienie Administratora Danych Osobowych wydane na podstawie aktualnego zakresu obowiązków zgodnie ze wzorem określonym w **załączniku nr 2** do Polityki Bezpieczeństwa.
2. Upoważnienie do przetwarzania danych osobowych dla pracowników Urzędu Gminy Secemin opracowuje pracownik wyznaczony przez Administratora Bezpieczeństwa Informacji, a podpisuje Administrator Bezpieczeństwa Informacji,
3. Pracownik wyznaczony przez Administratora Bezpieczeństwa Informacji prowadzi Ewidencje osób upoważnionych do przetwarzania danych osobowych. Ewidencja zawiera następujące informacje: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
4. Wzór Ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi **załącznik nr 6** do Polityki Bezpieczeństwa.
5. W przypadku zmiany zakresu czynności pracownika, do których został upoważniony na mocy wydanego upoważnienia, pracownik wyznaczony przez Administratora Bezpieczeństwa Informacji opracowuje nowe upoważnienie do przetwarzania danych osobowych.
6. Każdy pracownik przed dopuszczeniem go do przetwarzania danych osobowych, musi zostać przeszkolony w zakresie przepisów dotyczących ochrony danych osobowych oraz Polityki Bezpieczeństwa i Instrukcji.

2) OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH SĄ ZOBOWIĄZANE DO:

1. Bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych określonych w Polityce Bezpieczeństwa, Instrukcji i innych procedurach obowiązujących w Urzędzie Gminy Secemin.
2. Przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach).
3. Zabezpieczania zbiorów danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce Bezpieczeństwa, Instrukcji oraz innych procedurach obowiązujących w Urzędzie Gminy Secemin.
4. Niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie.
5. Nieudzielania informacji o danych osobowych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w takich przepisach zostały spełnione.
6. Niezwłocznego zawiadamiania Administratora Bezpieczeństwa Informacji o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

3) REJESTRACJA ZBIORÓW PRZETWARZANYCH PRZEZ ADMINISTRATORA DANYCH OSOBOWYCH W GIODO

1. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków:
    a. gdy dane przetwarzane w zbiorach, nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów danych zawierające dane wrażliwe,
    b. gdy powołał administratora bezpieczeństwa informacji i dokonał jego zgłoszenia do rejestracji Generalnemu Inspektorowi,

4) WEWNĘTRZNY REJESTR ZBIORÓW PRZETWARZANYCH PRZEZ ADMINISTRATORA DANYCH OSOBOWYCH

1. Rejestr zbiorów danych składa się z wykazu zbiorów danych osobowych przetwarzanych przez Urząd Gminy w Seceminie, zawierającego odrębnie dla każdego zbioru danych informacje określone w **załączniku nr 10**.
2. Rejestr prowadzony jest w postaci papierowej lub elektronicznej.
3. Za prowadzenie rejestru zgodnie z obowiązującymi przepisami i jego aktualizację odpowiada powołany przez administratora danych osobowych - Administrator Bezpieczeństwa Informacji.
4. Administrator bezpieczeństwa informacji w ramach prowadzenia rejestru dokonuje:
    a. wpisania zbioru danych w przypadku rozpoczęcia przetwarzania w nim danych osobowych;
    b. aktualizacji informacji dotyczących zbioru danych w przypadku zmiany informacji objętych wpisem;
    c. wykreślenia zbioru danych w przypadku zaprzestania przetwarzania w nim danych osobowych.

5. Wpisu do rejestru dokonuje się niezwłocznie po zaistnieniu zdarzenia, o którym mowa w ust. 4 pkt. a., powodującego obowiązek dokonania wpisu.
6. W rejestrze prowadzi się wykaz zmian, który zawiera:
    a. wskazanie rodzaju zmiany (nowy wpis, aktualizacja, wykreślenie);
    b. datę dokonania zmiany;
    c. zakres zmiany;
7. Administrator bezpieczeństwa informacji udostępnia rejestr do przeglądania przez udostępnienie rejestru na stronie internetowej administratora danych, pod adresem:
8. Wniosek o zarejestrowanie/zaktualizowanie w wewnętrznym rejestrze, zbioru danych osobowych wypełnia kierownik referatu, weryfikuje Administrator Bezpieczeństwa Informacji, a podpisuje Administrator Danych Osobowych.

IV. POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

W przypadku powierzania przetwarzania danych osobowych stosuje się wzór umowy, który stanowi załącznik nr 9 do Polityki Bezpieczeństwa.

V. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH.

1) ŚRODKI OCHRONY FIZYCZNEJ

1. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
2. 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.
3. Obszar przetwarzania danych osobowych określony w **załączniku nr 2** do Polityki Bezpieczeństwa zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
4. Pomieszczenia stanowiące obszar przetwarzania danych osobowych są zamykane na klucz. Każdy pracownik pobiera i zdaje klucze w sekretariacie, gdzie są one przechowywane w zamkniętej szafce.
5. Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych osobowych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

2) ŚRODKI SPRZĘTOWE, INFORMATYCZNE I TELEKOMUNIKACYJNE

1. Zastosowano kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią osobę wychodzącą i nie pozostawianiu pomieszczenia w czasie godzin pracy bez nadzoru.
2. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

3. Co najmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.
4. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych.
5. System operacyjny zapewnia odpowiednie restrykcje w zakresie dostępu do danych i aplikacji.
6. Zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed awarią zasilania.

3) ŚRODKI OCHRONY W RAMACH OPROGRAMOWANIA URZĄDZEŃ TELETRANSMISJI

1. Proces teletransmisji zabezpieczony jest za pomocą środków uwierzytelnienia.

4) ŚRODKI OCHRONY W RAMACH OPROGRAMOWANIA SYSTEMU

1. Zastosowano system operacyjny pozwalający na określenie odpowiednich praw dostępu do zasobów informatycznych dla poszczególnych użytkowników systemu informatycznego.
2. W systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł.
3. Serwery obsługujące bazę danych oraz stanowiska komputerowe służące do przetwarzania danych osobowych dostępne są wyłącznie po przeprowadzeniu prawidłowego procesu autoryzacji (system użytkowników i haseł, ograniczenie dostępu do poziomu poleceń systemowych lub zakaz wykonywania poleceń systemowych (restricted ShelI))
4. Zastosowano system rejestracji dostępu do zbioru danych osobowych.
5. Zastosowano oprogramowanie umożliwiające wykonanie kopii zapasowych zbiorów danych osobowych.
6. Zastosowano oprogramowanie zabezpieczające przed nieuprawnionym dostępem do systemu informatycznego - firewall, program antywirusowy.

5) ŚRODKI OCHRONY W RAMACH NARZĘDZI BAZ DANYCH I INNYCH NARZĘDZI PROGRAMOWYCH

1. Dostęp do zbioru danych osobowych zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano mechanizm umożliwiający rejestrację identyfikatora użytkownika wprowadzającego dane osobowe.
3. Wykorzystano środki pozwalające na rejestrację dokonanych zmian w zbiorze danych osobowych.
4. Zastosowano środki umożliwiające określenie praw dostępu do zbioru danych osobowych.
5. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji
6. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator,
7. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

6) ŚRODKI OCHRONY W RAMACH SYSTEMU UŻYTKOWEGO

1. Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
2. Zastosowano blokadę klawiatury, w przypadku dłuższej nieaktywnosci użytkownika.

7) ŚRODKI ORGANIZACYJNE

1. Przetwarzanie danych osobowych w Urzędzie Gminy Secemin może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
2. Opracowano I wdrożono Politykę Bezpieczeństwa i Instrukcję.
3. Wdrożono odpowiedni podział obowiązków i kontroli dostępu.
4. Do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych. Wzór upoważnienia stanowi **załącznik nr 4** do Polityki Bezpieczeństwa.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy.
6. Każdy pracownik podpisuje również oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami, którego wzór stanowi **załącznik nr 5** do Polityki Bezpieczeństwa.
7. Administrator Bezpieczeństwa Informacji prowadzi Ewidencję osób upoważnionych do przetwarzania danych osobowych.
8. Wprowadzono mechanizmy autoryzacji odpowiednio zabezpieczone przed dostępem osób trzecich.
9. Każdy pracownik Urzędu Gminy Secemin musi odbyć szkolenie w zakresie:
    - obwiązujących przepisów o ochronie danych osobowych. procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych.;
    - bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych.
    - Powyższy obowiązek dotyczy również każdego nowoprzyjętego pracownika, stażysty oraz ucznia będącego na praktykach. Za organizację szkoleń odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
10. Każdy upoważniony do przetwarzania danych osobowych potwierdza pisemnie fakt zapoznania się z treścią Polityki Bezpieczeństwa. Wzór oświadczenia stanowi **załącznik nr 7** do Polityki Bezpieczeństwa.
11. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom nieupoważnionym.
12. Tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w niszczarce.
13. Zapewniono klauzule poufności z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych.
14. Zapewnia się bezpieczne przechowywanie lub niszczenie uszkodzonych nośników zawierających dane osobowe (np. dysk twardy), szczególnie, gdy sprzęt, w którym zamontowany jest dany nośnik przekazywany jest do naprawy do firmy zewnętrznej.
15. Protokół przekazania przenośnego sprzętu komputerowego z obowiązkiem zwrotu stanowi **załącznik nr 2** do Instrukcji. Zgodę na użytkowanie komputera przenośnego (laptopa) poza siedzibą Urzędu Gminy Secemin wydaje Administrator Bezpieczeństwa Informacji.

VI. Postanowienia Końcowe

1. Wszelkie zmiany w ,,Polityce Bezpieczeństwa" wymagają zatwierdzenia przez Administratora Danych Osobowych.
2. Aktualizacje danych zawartych w załącznikach do „Polityki Bezpieczeństwa" będą dokonywane w miarę potrzeb, jednakże nie rzadziej niż raz do roku.

3. Odpowiedzialność karną za przetwarzanie danych osobowych niezgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, ze zm.) oraz przepisami wykonawczymi do tej ustawy określają art. 49-54 ww. ustawy.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z „Polityki Bezpieczeństwa" traktowane są jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w „Polityce Bezpieczeństwa", a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
5. Orzeczona kara dyscyplinarne wobec osoby uchylającej się od powiadomienia, nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku 0 ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, ze zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. Osoby, które zostały zapoznane z „Polityką Bezpieczeństwa" zobowiązują się do bezwzględnego stosowania zasad w niej zawartych.
7. Wszystkie regulacje określone w „Polityce Bezpieczeństwa" dotyczą przetwarzania danych osobowych w bazach prowadzonych w zarówno w formie elektronicznej jak i w formie papierowej.
8. W przypadku konieczności udostępnienia danych osobowych, Administrator Danych Osobowych udostępnia posiadane w zbiorze dane osobowe, osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
9. Dane osobowe mogą być udostępnione innym osobom niż wymienione w ust. 8, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
10. Dane osobowe udostępnia się na pisemny wniosek, chyba że przepis innej ustawy stanowi inaczej.
11. Udostępnione dane osobowe można wykorzystywać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
12. Niezależnie od zasad opisanych w „Polityce Bezpieczeństwa" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie, dokumenty te nie mogą być sprzeczne z regulacjami określonymi w „Polityce Bezpieczeństwa".