ZARZĄDZENIE NR 4 /2019
WÓJTA GMINY SIEMIATYCZE

z dnia 6 marca 2019 r.

w sprawie polityki bezpieczeństwa w Urzędzie Gminy Siemiatycze.

Na podstawie art.33 ust.3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2018r. poz. 994) i art. 24 ust.2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetawarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) , zarządzam, co następuje

§ 1. Wprowadza się do użytku służbowego:

1) Politykę Bezpieczeństwa Przetwarzania Danych Osobowych, która stanowi załącznik nr 1 do zarządzenia.

2) Instrukcję Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych, która stanowi załącznik nr 2 do zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Inspektorowi Ochrony Danych Osobowych

§ 3. Traci moc zarządzenie nr 15/2011 Wójta Gminy Siemiatycze z dnia 26 kwietnia 2011 roku w sprawie wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Gminie Siemiatycze.

§ 4. Zarządzenie wchodzi w zycie z dniem podpisania.

Wójt

Edward Krasowski

Załącznik Nr 1 do zarządzenia Nr 6/2019

Wójta Gminy Siemiatycze

z dnia 6 marca 2019 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY SIEMIATYCZE

Rozdział 1.
Postanowienia ogólne, definicje

§ 1.

1. Polityka Bezpieczeństwa w Urzędzie Gminy Siemiatycze jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Urząd Gminy Siemiatycze.

2. Celem Polityki bezpieczeństwa przetwarzania danych osobowych, zwanej dalej „Polityką bezpieczeństwa" w Urzędzie Gminy Siemiatycze jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

3. Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:

1) rozporządzeniu Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.1/,

2) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. .1000),

4. Przetwarzanie danych osobowych w Urzędzie Gminy Siemiatycze jest dopuszczalne wyłącznie pod warunkiem przestrzegania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/769 z dnia 27 kwietnia 2016 r, (RODO), ustawy z 10 maja 2018 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych w tym niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które powinny być spójne z polityką bezpieczeństwa wymaganą przez ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne.

5. Polityka Bezpieczeństwa ma zastosowanie do ochrony zbiorów danych osobowych i czynności w procesie przetwarzania danych osobowych w Urzędzie Gminy Siemiatycze, w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

§ 2.

1. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

2. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Organizacji rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych;

3. 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;

5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 3.

1. Administratorem danych osobowych przetwarzanych w Urzędzie Gminy Siemiatycze jest Wójt Gminy Siemiatycze

2. Administrator danych osobowych powołał inspektora ochrony danych, zgodnie art. 37 RODO. Zadania inspektora ochrony danych zawarte są w art. 39 RODO.

§ 4. Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1) administrator danych osobowych - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

2) inspektor ochrony danych - osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych;

3) ustawa - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000);

4) RODO - rozporządzenie Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/;

5) dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

6) dane biometryczne - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne

7) zbiór danych osobowych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów;

8) przetwarzane danych - operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.;

9) system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

10) system tradycyjny - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze;

11) zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

12) administrator systemu informatycznego - osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;

13) odbiorca - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia;

14) strona trzecia - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe;

15) identyfikator użytkownika (login) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

hasło - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym

Rozdział 2.
Obszary i zakres przetwarzania danych osobowych

§ 5.

1. Obszar przetwarzania danych osobowych w Urzędzie obejmuje budynek, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe (miejsca, w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje), oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).

2. Obszar przetwarzania danych osobowych określony jest w „Wykazie pomieszczeń, w których przetwarzane są dane osobowe", stanowiącym załącznik nr 1 do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Siemiatycze. Wykaz ten zawiera następujące informacje:

1) lokalizację budynku;

2) numer pomieszczenia i jego przeznaczenie;

3) wskazanie piętra budynku;

4) określenie referatu użytkującego dane pomieszczenie;

5) wskazanie liczby osób pracujących w pomieszczeniu

6) określenie zabezpieczenia pomieszczenia.

3. Obszar przetwarzania danych oraz warunki ochrony tego obszaru określone zostały w załączniku nr 2 do Polityki Bezpieczeństwa „Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe".

§ 6.

1. Wykaz zbiorów danych przetwarzanych w Urzędzie Gminy określony został w załączniku nr 3 do Polityki Bezpieczeństwa - „Wykaz zasobów danych osobowych i systemów ich przetwarzania". Wykaz ten zawiera następujące informacje:

1) nazwę zbioru danych;

2) określenie systemu przetwarzania danych osobowych;

3) lokalizację miejsca przetwarzania danych osobowych;

4) stosowane przy przetwarzaniu danych osobowych oprogramowanie;

5) precyzyjny zakres danych osobowych w systemie (pola i relacje pomiędzy nimi);

6) określenie pól informacyjnych w systemie;

7) określenie sposobu przepływu danych pomiędzy systemami;

2. wskazanie możliwość wydruku zakresu przetwarzania danych osobowych. Szczegółowe informacje dotyczące stosowanego sprzętu oraz oprogramowania danego systemu informatycznego są zawarte w instrukcjach zarządzania systemem. Działające systemy to programy dziedzinowe.

§ 7.

1. W Urzędzie przetwarzane są dane osobowe kandydatów do pracy, pracowników, członków rodzin pracowników, kierowanych do prac społecznie użytecznych,, stażystów, praktykantów, mieszkańców, klientów, kierowanych do Gminnej Komisji Rozwiązywania Problemów Alkoholowych, osób korzystających z kolonii letnich, wycieczek, uczniów uczestniczących w programach, projektach zebrane w zbiorach danych osobowych.

2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.

3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

4. Innymi dokumentami regulującymi ochronę danych osobowych w Urzędzie są:

1) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Organizacji;

2) ewidencja osób upoważnionych do przetwarzania danych osobowych;

3) rejestr czynności przetwarzania danych osobowych;

4) procedura postępowania w przypadku naruszenia ochrony danych osobowych;

5) rejestr kategorii przetwarzania danych;

6) ewidencja zawartych umów powierzenia przetwarzania danych osobowych;

7) klauzula informacyjna.

5. Politykę bezpieczeństwa stosuje się w szczególności do:

1) danych osobowych przetwarzanych w systemach dziedzinowych

2) wszystkich informacji dotyczących danych kandydatów do pracy, pracowników, członków rodzin pracowników, kierowanych do prac społecznie użytecznych,, stażystów, praktykantów, mieszkańców, klientów, kierowanych do Gminnej Komisji Rozwiązywania Problemów Alkoholowych, osób korzystających z kolonii letnich, wycieczek, uczniów uczestniczącychw programach, projektach;

3) odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia;

4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;

5) rejestru osób trzecich mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych;

6) innych dokumentów zawierających dane osobowe.

§ 8.

Przetwarzanie danych osobowych odbywa się na serwerze i na stacjach roboczych użytkowników.

§ 9.

1. W ramach procesów przetwarzania danych ma miejsce przepływ danych pomiędzy różnymi systemami informatycznymi. Informacje na temat przepływu danych pomiędzy różnymi systemami informatycznymi znajdują się w „Wykazie zasobów danych osobowych i systemów ich przetwarzania, o którym mowa w § 4 ust. 5 pkt 1".

2. Szczegółowe informacje dotyczące przepływu danych osobowych pomiędzy danymi systemami informatycznymi znajdują się w instrukcjach zarządzania danym systemem.

§ 10.

1. W systemie informatycznym obowiązują zabezpieczenia na poziomie podstawowym. Szczegółowe omówienie środków zabezpieczenia technicznego i organizacyjnego znajduje się w „Instrukcję Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych", stanowiącej załącznik nr 2 do Zarządzenia Wójta Gminy Siemiatycze z dnia 0 2018 r.

2. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;

2) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

3) wszystkich pracowników, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie.

3. Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy, stażyści, praktykanci oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

Rozdział 3.
Zarządzanie przetwarzaniem danych osobowychoraz czuwanie nad ich bezpieczeństwem

§ 11. ADO powołuje Administratora Systemów Informatycznych jako zarządzającego oprogramowaniem, który przeprowadza okresową inwentaryzację oprogramowania oraz ustanawia zasady i procedury ciągłego utrzymania oprogramowania.

§ 12. W celu realizacji powierzonych zadań IOD w Urzędzie ma prawo:

1) kontrolować komórki organizacyjne Urzędu w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
2) wydawać polecenia kierownikom komórek organizacyjnych Urzędu w zakresie bezpieczeństwa danych osobowych;
3) informować ADO o przypadkach naruszenia bezpieczeństwa danych osobowych;
4) żądać od wszystkich pracowników Urzędu wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

§ 13. . Wójt wyznacza właścicieli zasobów danych osobowych.

2. Rolę właścicieli zasobów danych osobowych pełnią kierownicy referatów odpowiedzialni za dany zasób danych osobowych.

3. Do obowiązków właścicieli zasobów danych osobowych należy w szczególności:

1) zarządzanie zasobem danych osobowych w ramach zadań realizowanych przez kierowane referaty;
2) występowanie z wnioskiem do ADO o nadanie upoważnień dotyczących dostępu do zasobu danych osobowych podległym pracownikom;
3) zgłaszanie do IOD zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru;
4) udostępnianie danych osobowych innemu podmiotowi lub osobie, której dane dotyczą;
5) przestrzeganie obowiązków dotyczących obszaru przetwarzania, wykazu osób upoważnionych do przetwarzania danych osobowych, zastosowania zabezpieczeń zbiorów;
6) prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w kierowanym referacie, z uwzględnieniem zakresu odpowiedzialności za ochronę tych danych w stopniu odpowiednim do zadań wykonywanych przez te osoby przy przetwarzaniu danych osobowych i przekazywanie IOD aktualnej ewidencji tych osób wraz z priorytetami im przydzielonymi;
7) zapoznawanie pracowników mających dostęp do danych osobowych z przepisami

   dotyczącymi ochrony danych osobowych

§ 14. 1. Administrator Systemu Informatycznego odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu.

2. Do obowiązków ASI w zakresie ochrony danych osobowych należy w szczególności:

1) zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie;
2) nadzór nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
3) nadzór nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych;
4) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Urzędzie w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych;
5) monitorowanie przesyłania danych osobowych drogą teletransmisji;
6) nadzór nad przestrzeganiem zasad bezpieczeństwa w przypadku udostępniania danych osobowych innym podmiotom drogą teletransmisji danych;

7) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

8) podejmowanie działań w przypadku naruszeń w systemie zabezpieczeń;

9) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

10) podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.

Rozdział 4.
Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 15.

1. W ramach zabezpieczenia organizacyjnego wykonano następujące zadania:

1) opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych;

2) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie;

3) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;

4) opracowano i na bieżąco prowadzi się rejestr czynności przetwarzania;

5) opracowano i upubliczniono klauzule informacyjną, zawarto umowy z firmami informatycznymi sprawującymi nadzór nad programami użytkowanymi w urzędzie;

6) wyznaczono inspektora ochrony danych;

7) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną;

8) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;

9) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;

10) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;

11) 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;

2. dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.W ramach zabezpieczenia technicznego wykonano następujące zadania:

1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą programu zabezpieczającego (FireWall sprzętowy i systemowy)

2) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową;

3) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła.

3. W ramach środków ochrony fizycznej wykonano następujące zadania:

1) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem;

2) dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach;

3) urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach.

Rozdział 5.
Gromadzenie danych

§ 16.

Dane osobowe przetwarzane w Urzędzie mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa

§ 17.

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 18.

W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem rozporządzenia lub ustawy, albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział 6.
Obowiązek informacyjny

§ 19. Kierownicy komórek organizacyjnych Urzędu, w których są zbieranie i przetwarzane dane osobowe, są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają w zakresie określonym w art. 12-14 rozporządzenia (RODO).

§ 20. 1. Materiały dotyczące innej niż ustawowa działalności Urzędu mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.

2. Kandydaci do pracy w Urzędzie w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.

3. Dokumenty złożone w celu określonym w ust. 2 są przechowywane w komórce organizacyjnej, która przetwarza te dane, i są włączane do akt osobowych pracownika.

4. Klauzule informacyjne Administrator Danych zamieszcza w Biuletynie Informacji Publicznej oraz wywiesza na tablicy ogłoszeń Urzędu Gminy .

Rozdział 7.
Udostępnianie danych osobowych

§ 21.

1. . ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

2. Dane osobowe mogą być udostępniane w następujących przypadkach:

1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;

2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;

3) na podstawie wniosku osoby, której dane dotyczą.

3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi załącznik nr 6 do Polityki Bezpieczeństwa.

4. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

5. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.

6. Właściciel zasobów danych osobowych jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

7. Prawo dostępu przysługujące osobie, której dane dotyczą jest realizowane zgodnie z przepisami art. 15 rozporządzenia(RODO)

§ 22. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy

Rozdział 8.
Ochrona przetwarzania danych osobowych

§ 23. .

1. Do przetwarzania danych mogą być dopuszczeni pracownicy Urzędu posiadający upoważnienie nadane przez ADO.

2. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

§ 24. ADO zobowiązany jest do zbierania, ewidencjonowania i przechowywania:

1) oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych;

2) oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy;

3) porozumień, umów zawartych z osobami zatrudnionymi przy przetwarzaniu danych osobowych w zakresie wykorzystania oddanego im do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej.

§ 25. 1. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy zawartej na piśmie pomiędzy ADO a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.

2. Właściciel zasobów danych osobowych informuje IOD o zamiarze powierzenia danych osobowych do przetwarzania.

3. IOD przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.

4. W projekcie umowy należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.

5. Każda osoba delegowana do wykonywania zadań na rzecz Urzędu Gminy, związanych z powierzeniem przetwarzania danych osobowych, obowiązana jest podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.

§ 26.

1. Podmiot przetwarzający dane osobowe jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.

2. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.

3. Podmiot przetwarzający dane osobowe ponosi odpowiedzialność za ochronę przetwarzanych danych osobowych.

Rozdział 9.
Postępowanie w przypadkach naruszenia ochrony danych osobowych

§ 27. Przepisy niniejszego rozdziału stosuje się w przypadku:

1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych;

2) podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.

§ 28. Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

§ 29. Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych;

2) nieautoryzowane modyfikacje lub zniszczenie danych;

3) udostępnienie danych nieautoryzowanym podmiotom nielegalne ujawnienie danych;

4) pozyskiwanie danych z nielegalnych źródeł.

§ 30.

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego lub IOD , a następnie postępować stosownie do podjętej przez niego decyzji.

2.

Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:

1) opisanie działania wskazującego na naruszenie ochrony danych osobowych;

2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;

3) wskazanie istotnych informacji mogących wskazywać na przyczynę naruszenia;

4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ 31. Administrator Danych jest zobowiązany zapewnić odpowiedni stopień bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy uwzględniając postanowienia zawarte w art. 32 rozporządzenia (RODO)

§ 32. W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki zgłoszą naruszenie organowi nadzorczemu. Sposób postępowania w przypadku naruszenia ochrony danych osobowych określają przepisy art. 33 i art. 34 rozporządzenia (RODO).

Rozdział 10.
Zadania administratora danych osobowych lub inspektora ochrony danych

§ 33. Do najważniejszych obowiązków administratora danych osobowych lub administratora bezpieczeństwa informacji należy:

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych;

2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa i innymi dokumentami wewnętrznymi;

3) przeprowadzenie oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych - w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych;

4) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;

5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

6) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych

7) nadzór nad bezpieczeństwem danych osobowych;

8) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;

inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

Rozdział 11.
Zadania administratora systemu informatycznego -informatyka urzędu

§ 34.

1. Administrator systemu informatycznego odpowiedzialny jest za:

1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;

2) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego;

3) instalacje i konfiguracje oprogramowania systemowego, sieciowego;

4) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem;

5) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;

6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;

7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego;

8) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie;

9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;

10) przyznawanie na wniosek administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie;

11) wnioskowanie do administratora danych osobowych lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;

12) zarządzanie licencjami, procedurami ich dotyczącymi;

13) prowadzenie profilaktyki antywirusowej.

2.

Praca administratora systemu informatycznego jest nadzorowana pod względem przestrzegania RODO, ustawy o ochronie danych osobowych, oraz Polityki bezpieczeństwa i przez administratora danych lub inspektora ochrony danych.

Rozdział 12.
Postanowienia końcowe

§ 35. 1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych lub inspektor ochrony danych.

3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych,

Szkolenie zostaje zakończone podpisaniem przez uczestnika oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych

Załącznik Nr 2 do zarządzenia Nr 6/2019

Wójta Gminy Siemiatycze

z dnia 6 marca 2019 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Rozdział 1.
Procedury nadawania uprawnień do przetwarzania danychi rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 1. 1.

. Użytkownikowi zostaje przyznany unikalny w konkretnym podsystemie identyfikator wraz z poufnym hasłem, który proponuje Administrator systemu informatycznego występując z wnioskiem o przyznanie użytkownikowi uprawnień do przetwarzania danych w podsystemie.

2. O przyznaniu identyfikatora decyduje Administrator Danych Osobowych, co jest tożsame z przyznaniem użytkownikowi prawa do przetwarzania danych osobowych w systemie informatycznym.

3. Identyfikator wraz z prawidłowym hasłem umożliwia użytkownikowi dostęp do podsystemu przetwarzania danych osobowych.

4. Każdy z użytkowników przed dopuszczeniem do podsystemu podpisuje umowę o zachowaniu poufności, zapoznaje się z Instrukcją Zarządzania i Polityką Bezpieczeństwa oraz zostaje pouczony o wdrożonych procedurach bezpieczeństwa.

5. Administratorowi systemu informatycznego przysługuje prawo do zablokowania konta użytkownika w każdym czasie.

6. Po zakończeniu operacji w systemie informatycznym, użytkownik zobowiązany jest wylogować się z podsystemu

7. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych – każdy użytkownik zobowiązany jest do niezwłocznego powiadomienia Administratora Danych lub Administratora systemu informatycznego

8. Użytkownikom przyznaje się równe uprawnienia w dostępie do podsystemu (poziom podstawowy) chyba, że specyfika systemu wymaga innego podejścia

Rozdział 2.
Stosowane metody i środki uwierzytelnieniaoraz procedury związane z ich zarządzaniem i użytkowaniem

§ 2.

1. Użytkownicy którym przyznano dostęp do podsystemu przetwarzania danych osobowych (w tym identyfikator dostępu do systemu) ustalają hasło dostępu z Administratorem systemu informatycznego

2. Hasło jest informacją o poufnym charakterze i należy zachować je w tajemnicy

3. Obowiązuje ścisły zakaz ujawniania hasła osobom trzecim, w tym innym użytkownikom.

4. Hasła do wszystkich podsystemów użytkowanych w Zakładzie/Dziale należy przechowywać w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem

5. .Osobą odpowiedzialną za bezpieczne przechowywanie listy identyfikatorów wraz z hasłami wymienionymi w pkt. 4 jest Administrator systemu informatycznego

6. Dostęp do listy identyfikatorów i haseł użytkowników wszystkich użytkowanych podsystemów posiada Administrator systemu informatycznego. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie Administratorowi systemu informatycznego.

§ 3.

1. Hasło składa się z ciągu co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasła są różne dla każdego z użytkowników.

3. Hasła są przechowywane w podsystemie w postaci zaszyfrowanej.

4. Para „identyfikator i hasło" przyznane jednemu użytkownikowi nie może zostać powtórnie wykorzystane.

5. Hasła są zmieniane nie rzadziej niż co 30 dni.

6. System wymusza zmianę hasła.

7. Użytkownik zobowiązany jest zapamiętać hasło, o którym mowa wyżej.

8. Jeżeli system informatyczny środkami technicznymi nie wymusza podjęcia czynności określonych w pkt 1-6, użytkownik zobowiązany jest do przestrzegania powyższych zasad, a tym samym do okresowej zmiany hasła i ustanowieniu nowego, spełniającego wymogi określone w niniejszym paragrafie.

9. Alternatywnie użytkownik może zamiast hasła logować się do urządzeń za pomocą czytnika linii papilarnych.

§ 4. Osobą odpowiedzialną za ustalanie poprawności haseł jest Administrator systemu informatycznego. Jeśli użytkownik podsystemu odpowiedzialny za zmianę hasła nie jest pewien jego poprawności, zobowiązany jest do konsultacji z osobą odpowiedzialną za ustalanie poprawności bezpiecznych haseł

Rozdział 3.
Procedury rozpoczęcia, zawieszenia i zakończenia pracyprzeznaczone dla użytkowników systemu

§ 5. 1. W celu uruchomienia podsystemu informatycznego użytkownik powinien:

1) uruchomić komputer,

2) wybrać odpowiednią opcję umożliwiającą logowanie do podsystemu,

3) zalogować się do podsystemu poprzez wskazanie loginu oraz poufnego i aktualnego hasła.

4) alternatywnie zalogować się poprzez użycie czytnika linii papilarnych

2. Użytkownik podczas logowania do podsystemu nie może ujawniać hasła osobom trzecim w tym innym administratorom oraz pozostawiać zapisanego hasła w pobliżu stanowiska pracy i innych pracowników.

3. Użytkownik zobligowany jest do skutecznego wylogowania się z podsystemu za każdym razem, gdy zamierza opuścić stanowisko pracy, niezależnie od tego na jak długo ma zamiar odejść od komputera.

4. Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj" lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie bez znajomości hasła, dzięki zastosowaniu funkcji wygaszacza ekranu.

5. Ekrany komputerów, na których przetwarzane są dane osobowe, należy chronić wygaszaczami zabezpieczonymi hasłem. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych.

6. W przypadku stwierdzenia fizycznej ingerencji w systemie lub innych podejrzeń dotyczących możliwości naruszenia bezpieczeństwa systemu, użytkownik niezwłocznie zawiadamia o zaistniałym fakcie Administratora systemu informatycznego lub bezpośrednio Inspektora Ochrony Danych.

Rozdział 4.
Procedury tworzenia kopii zapasowych zbiorów danychoraz programów i narzędzi programowych służących do ich przetwarzania

§ 6. 1. Kopie zapasowe zbiorów danych osobowych tworzone są codziennie po zakończonym dniu pracy ze zbiorem, chyba że danego dnia nie dokonano żadnych zmian w zbiorze.

2. Za tworzenie kopii zapasowych odpowiedzialny jest Administrator systemu informatycznego.

3. Administrator systemu informatycznego dokonuje zapisu kopii zbiorów danych osobowych na serwerze plików sieci lokalnej.

4. Administrator systemu informatycznego oznacza i przechowuje kopie zbiorów danych w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem.

5. Poprawność procesu tworzenia i przechowywania kopii zapasowych – nadzoruje Administrator systemu informatycznego

Rozdział 5.
Sposób, miejsce i okres przechowywania elektronicznych nośników informacjizawierających dane osobowe oraz kopii zapasowych

§ 7.

1. Elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamkniętych szafkach z zabezpieczeniem dostępu osób trzecich.

2. Kopie bezpieczeństwa są niezwłocznie zniszczone po ustaniu użyteczności danych osobowych tam zawartych.

3. Zniszczenia kopii dokonuje się w sposób uniemożliwiający późniejsze odtworzenie danych, poprzez fizyczne zniszczenie nośników danych lub jeśli to niemożliwe, poprzez trwałe usunięcie danych przy pomocy specjalistycznego oprogramowania służącego do tego celu. W przypadku wątpliwości, należy zwrócić się do Inspektora Ochrony Danych.

4. Fakt zniszczenia kopii zapasowych wymaga sporządzenia na tę okoliczność protokołu opatrzonego podpisem Inspektora Ochrony Danych i osoby sporządzającej ten dokument.

5. Czas przechowywania kopii zapasowych zależy od aktualaności zapisanych danych oraz potrzeby tworzenia kolejnych kopii. Jeżeli przepisy nie stanowią inaczej na czas przechowywania kopii zapasowych nalezy ograniczyć do:

1) tygodniowych - 1 miesiąc;

Rozdział 6.
Sposób zabezpieczenia systemu informatycznego

§ 8.

1. System informatyczny Urzędy jest zabezpieczony przed atakami z zewnątrz sieci za pomocą oprogramowania typu firewall. Dodatkowo na serwerze pocztowym program antywirusowy chroni system przed przedostaniem się do wewnątrz sieci złośliwego oprogramowania.

2. Komponenty serwerowe chronione są przed zakłóceniami w sieci zasilającej przy pomocy urządzeń typu UPS, podtrzymujących zasilanie.

3. Każdy podsystem w którym ma miejsce przetwarzanie danych osobowych, podlega ochronie przed działaniem wirusów komputerowych aktualnym oprogramowaniem antywirusowym aktualizowanym na bieżąco.

4. W celu przeciwdziałania atakom zainfekowanych plików, podsystem musi być skanowany przynajmniej raz dziennie pod kątem obecności w systemie wirusów i innych zagrożeń. Za proces ten odpowiedzialny jest Administrator systemu informatycznego.

5. W przypadku wykrycia jakiegokolwiek zagrożenia użytkownik niezwłocznie zawiadamia Administratora systemu informatycznego.

6. Wszystkie komputery, na których uruchomione są podsystemy przetwarzające dane osobowe muszą być zaopatrzone w urządzenia typu UPS, podtrzymujące zasilanie, a tym samym zabezpieczające podsystem przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

7. W przypadku stwierdzenia braku zasilania należy dokonać natychmiastowego zapisu danych osobowych oraz przeprowadzić procedurę opuszczenia podsystemu.

§ 9.

1. Podsystemy informatyczne nie służące do przetwarzania danych osobowych, a ograniczone wyłącznie do edycji tekstu w celu udostępnienia go na piśmie, zapewniają odnotowanie:

1) informacji o odbiorcach, którym dane osobowe zostały udostępnione,

2) dacie i zakresie tego udostępnienia.

2. Odnotowanie następuje przez automatyczny zapisek okoliczności w podsystemie.

Rozdział 7.
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacjisłużących do przetwarzania danych osobowych

§ 10.

1. Przeglądów oraz konserwacji systemu dokonuje Administrator systemu informatycznego.

2. W przypadku przekazania innym podmiotom elementów systemu w celu naprawy, wszelkie dane osobowe muszą zostać z nich usunięte. Proces ten nadzoruje Administrator systemu informatycznego.

3. Dane osobowe muszą być zabezpieczone przed dostępem osób trzecich zanim nośnik lub element systemu zostanie przekazany podmiotowi innemu niż Administrator systemu informatycznego lub Inspektor Ochrony Danych.