WÓJT GMINY
Nowogródek Pom.
woj. zachodniopomorskie

RO.0050.64.2019.ZW

ZARZĄDZENIE NR 64/2019
WÓJTA GMINY NOWOGRÓDEK POMORSKI
z dnia 09 września 2019 r.

w sprawie wprowadzenia „Polityki ochrony danych" w Urzędzie Gminy Nowogródek Pomorski.

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (tj. Dz. U. z 2018r., poz. 994) oraz art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE, L 119 z 4.05.2016 t.) zarządzam, co następuje:

§ 1.

Wprowadza się w Urzędzie Gminy Nowogródek Pomorski „Politykę ochrony danych", stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Wykonanie Zarządzenia powierzam Inspektorowi Ochrony Danych.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Krzysztof Mrzygłód

Załącznik do Zarządzenia Nr 64/2019
Wójta Gminy Nowogródek Pomorski
z dnia 09 września 2019 r.

Polityka ochrony danych w Urzędzie Gminy Nowogródek Pomorski

Rozdział 1
Postanowienia ogólne

§ 1.

Celem Polityki ochrony danych w Urzędzie Gminy Nowogródek Pomorski, zwanym dalej „Organizacją", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane, w tym również dane osobowe.

§ 2.

Polityka ochrony danych została opracowana w oparciu o wymagania zawarte w: • 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/, • Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 24 maja 2018 r., poz. 1000), • Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r., poz. 2247), • ustawie z dnia 9 lutego 2018 r. o ochronie informacji niejawnych (tj. Dz. U. z 2018r., poz. 412) • Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125).

§ 3.

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

§ 4.

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

§ 5.

1. Administratorem jest Urząd Gminy Nowogródek Pomorski reprezentowany przez Wójta Gminy Nowogródek Pomorski.
2. Administrator powołał Inspektora Ochrony Danych (IOD), zgodnie art. 37 RODO, którym jest Carlo Paolicelli, Zastępca Wójta Gminy Nowogródek Pomorski. Zadania IOD zawarte są w art. 39 RODO.

Rozdział 2
Definicje

§ 6.

Przez użyte w Polityce ochrony danych określenia należy rozumieć:

1. **Administrator danych** – zwany dalej Administratorem lub AD, jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych, w tym danych osobowych,
2. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora, nadzorująca przestrzeganie zasad i wymogów ochrony danych określonych w RODO i przepisach krajowych,
3. **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 24 maja 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** – wszelkie informacje, w tym również dane osobowe, przetwarzane w Organizacji w sposób tradycyjny, jak również za pomocą systemu informatycznego,
6. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
7. **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
8. **przetwarzane danych** – operacja lub zestaw operacji wykonywanych na danych 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,
10. **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych na papierze,
11. **system zarządzania bazą danych,** zwany dalej systemem - oprogramowanie służące do zarządzania bazą danych (moduły programowe) przetwarzające dane zawarte w jednym lub wielu zbiorach.
12. **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
13. **Administrator systemu informatycznego (ASI)** – osoba lub osoby, upoważnione przez Administratora do administrowania i zarządzania systemem informatycznym,

14. **odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
15. **strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia Administratora mogą przetwarzać dane osobowe,
16. **identyfikator użytkownika** (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym,
17. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3 Zakres stosowania

§ 7.

1. W Organizacji przetwarzane są dane zebrane w zbiorach danych, ale również dane bez wyraźnego usystematyzowania.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka ochrony danych zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych.
4. Innymi dokumentami w Organizacji regulującymi ochronę danych, w tym również osobowych, są:
   1. instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych, 2. ewidencja osób upoważnionych do przetwarzania danych,
   3. instrukcja zarządzania incydentami,
   4. instrukcja postępowania w przypadku naruszenia ochrony danych,
   5. rejestr czynności przetwarzania danych,
   6. instrukcja przetwarzania danych w imieniu Administratora.

§ 8.

Politykę ochrony danych stosuje się w szczególności do:
   1. danych przetwarzanych w Systemach: ŹRÓDŁO, Dowody Osobiste, ELUD, BeSTi@ SJO, GEO-INFO 7, Kadry i Płace, Płatnik, Woda i Ścieki – szczegółowy wykaz Systemów zawiera Załącznik nr 4 do „Polityki bezpieczeństwa przetwarzania danych", wprowadzonej odrębnym zarządzeniem,
   2. wszystkich informacji dotyczących danych pracowników Administratora, mieszkańców Gminy Nowogródek Pomorski,
   3. odbiorców danych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia, którymi są m.in. lekarz medycyny pracy, obsługa prawna, obsługa informatyczna, obsługa BHP,
   4. informacji dotyczących zabezpieczenia danych, w tym w szczególności nazw kont i haseł w systemach służących do przetwarzania danych,
   5. rejestru osób, którym Administrator nadał upoważnienia do przetwarzania danych,
   6. innych dokumentów zawierających dane.

§ 9.

1. Zakresy ochrony danych określone przez Politykę ochrony danych oraz inne z nią związane dokumenty mają zastosowanie do:
   1. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów oraz tych w formie tradycyjnej, 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, zleceniobiorców, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez Politykę ochrony danych oraz inne z nią związane dokumenty zobowiązani są wszystkie wymienione wyżej grupy osób oraz inne osoby mające dostęp do danych podlegających ochronie.

Rozdział 4
Wykaz zbiorów danych, w tym danych osobowych

§ 10.

Dane gromadzone są w zbiorach:
1. KONTRAHENCI
2. DOWODY OSOBISTE
3. PODATKI I OPŁATY LOKALNE
4. STYPENDIA
5. REJESTR OSÓB UZALEŻNIONYCH OD ALKOHOLU
6. EWIDENCJA GRUNTÓW I BUDYNKÓW
7. AKCYZA PALIWOWA
8. ZARZĄDZANIE NIERUCHOMOŚCIAMI
9. KWALIFIKACJA WOJSKOWA
10. ŚWIADCZENIA OSOBISTE I RZECZOWE
11. SYSTEM INFORMACJI OŚWIATOWEJ
12. EWIDENCJA DZIAŁALNOŚCI GOSPODARCZEJ
13. EWIDENCJA PRACOWNIKÓW
14. EWIDENCJA OSÓB UBEZPIECZONYCH W ZUS
15. BUDOWNICTWO
16. EWIDENCJA LUDNOŚCI
17. OPŁATA ŚMIECIOWA
18. ZEZWOLENIA NA SPRZEDAŻ I PODAWANIE NAPOJÓW ALKOHOLOWYCH
19. SPRAWY WOJSKOWE I OBRONY CYWILNEJ
20. PRZELEWY BANKOWE
21. BAZA NOCLEGOWA
22. REJESTR KORESPONDENCJI PRZYCHODZĄCEJ
23. OŚWIADCZENIA MAJĄTKOWE
24. WODA I ŚCIEKI
25. POCZTA ELEKTRONICZNA
26. REJESTR CZYNNOŚCI PRZETWARZANIA I EWIDENCJA OBOWIĄZKU INFORMACYJNEGO

§ 11.

Zbiory danych wymienione w § 10 ust. 1 pkt 6, 8, 9, 10, 11, 16, 19, 20, 22, 25 podlegają przetwarzaniu w sposób tradycyjny, a zbiory określone w pkt 1, 2, 3, 4, 5, 7, 12, 13, 14, 15, 17, 18, 21, 23, 24, 26, 27, 28 gromadzone są i przetwarzane przy użyciu systemów – Załącznik nr 6 do „Polityki bezpieczeństwa przetwarzania danych", wprowadzonej odrębnym zarządzeniem.

Rozdział 5
Wykaz budynków, pomieszczeń, w których wykonywane są operacje przetwarzania danych

§ 12.

1. Dane, w tym dane osobowe, przetwarzane są w budynku, mieszczącym się w Nowogródku Pomorskim przy ulicy Mickiewicza 15.
2. Obszar, w którym przetwarzane są dane za pomocą systemów oraz tradycyjnie, w których przechowuje się wszelkie nośniki informacji zawierające dane, jak również te podlegające zniszczeniu stanowi Załącznik nr 2 do „Polityki bezpieczeństwa przetwarzania danych", wprowadzonej odrębnym zarządzeniem.

Rozdział 6
Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

§ 13.

Wykaz zbiorów danych wraz ze wskazaniem systemów zastosowanych do przetwarzania tych danych zawiera Załącznik nr 3 do „Polityki bezpieczeństwa przetwarzania danych", wprowadzonej odrębnym zarządzeniem.

Rozdział 7
Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych

§ 14.

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych zawarta jest w Załączniku nr 4 do „Polityki bezpieczeństwa przetwarzania danych", wprowadzonej odrębnym zarządzeniem.

Rozdział 8
Sposób przepływu danych między poszczególnymi systemami, współpracy systemów ze zbiorami danych.

§ 15.

Przepływ danych pomiędzy poszczególnymi Systemami zawiera Załącznik nr 5 do „Polityki bezpieczeństwa przetwarzania danych", wprowadzonej odrębnym zarządzeniem.

Rozdział 9
Środki organizacyjne i techniczne zabezpieczenia danych

§ 16.

1. Zabezpieczenia organizacyjne:
    1. opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych,
    2. sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych w Organizacji,
    3. stworzono procedurę postępowania w sytuacji naruszenia ochrony danych,
    4. opracowano i bieżąco prowadzi się rejestr czynności przetwarzania,
    5. opracowano i wdrożono instrukcję posługiwania się pocztą elektroniczną,
    6. wyznaczono Inspektora Ochrony Danych,
    7. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora bądź osobę przez niego upoważnioną,
    8. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych oraz w zakresie zabezpieczeń Systemu Informatycznego,
    9. osoby zatrudnione przy przetwarzaniu danych obowiązane zostały do zachowania ich w tajemnicy,
    10. przetwarzanie danych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
    11. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych oraz w warunkach zapewniających bezpieczeństwo danych,
    12. dokumenty i nośniki informacji zawierające dane, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

2. Zabezpieczenia techniczne:
   1. wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą urządzenia UTM,
   2. stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
   3. komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanej zmiany hasła,

3. Środki ochrony fizycznej:
   1. obszar, na którym przetwarzane są dane, poza godzinami pracy, chroniony jest alarmem,
   2. urządzenia służące do przetwarzania danych umieszczone są w zamykanych pomieszczeniach,
   3. dokumenty i nośniki informacji zawierające dane przechowywane są w zamykanych na klucz szafach.

Rozdział 10
Zadania Administratora lub Inspektora Ochrony Danych

§ 17.

1. Do najważniejszych obowiązków Administratora lub IOD należy:
   1. organizacja bezpieczeństwa i ochrony danych 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 – w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych, 4. wydawanie i anulowanie upoważnień do przetwarzania danych,
   5. prowadzenie ewidencji osób upoważnionych do przetwarzania danych,
   6. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
   7. nadzór nad bezpieczeństwem danych,
   8. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
   9. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych.

Rozdział 11
Zadania Administratora Systemu Informatycznego

§ 18.

1. ASI 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,

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 lub IOD ściśle określonych praw dostępu do informacji w Systemach,
11. wnioskowanie do Administratora lub IOD w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
12. zarządzanie licencjami, procedurami ich dotyczącymi,
13. prowadzenie profilaktyki antywirusowej.

2. Praca ASI jest nadzorowana pod względem przestrzegania RODO, ustawy o ochronie danych osobowych, oraz Polityki ochrony danych Organizacji przez Administratora lub IOD.

Rozdział 12
Sprawozdanie roczne z funkcjonowania systemu ochrony danych

§ 19.

1. Corocznie do dnia 31 grudnia IOD przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych i przekazuje do Administratora.
2. Sprawozdanie przygotowywane jest w formie pisemnej.

Rozdział 13
Postanowienia końcowe

§ 20.

1. Każdy użytkownik przed dopuszczeniem do pracy z Systemem przetwarzającym dane lub zbiorami danych w formie tradycyjnej winien być poddany przeszkoleniu w zakresie ochrony danych.
2. Za przeprowadzenie szkolenia odpowiada Administrator lub IOD.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami RODO, ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką ochrony danych i innymi związanymi z nią dokumentami obowiązującymi u Administratora.
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych.