POLITYKA BEZPIECZEŃSTWA

Administrator Danych Osobowych – **Burmistrz Miasta i Gminy Frombork**

dnia 23 marca 2016 roku w podmiocie o nazwie: **Urząd Miasta i Gminy we Fromborku,**

zgodnie z **ROZPORZĄDZENIEM 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)
wdraża dokument o nazwie Polityka Bezpieczeństwa.

§ 1. Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w podmiocie: **Urząd Miasta i Gminy we Fromborku**, **ul. Młynarska 5a, 14-530 Frombork**, określa zasady przetwarzania danych osobowych, oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka Bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka Bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych, oraz w systemach informatycznych.

§ 2. Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1. **ZBIORZE DANYCH** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. **PRZETWARZANIU DANYCH** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. **SYSTEMIE INFORMATYCZNYM** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. **ZABEZPIECZENIU DANYCH W SYSTEMIE INFORMATYCZNYM** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. **USUWANIU DANYCH** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. **ADMINISTRATORZE DANYCH OSOBOWYCH** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (t.j. Dz. U. 2014 r., poz. 1182, zm. poz. 1662 oraz z 2015 r. poz. 1309.), decydujące o celach i środkach przetwarzania danych osobowych,
7. **ADMINISTRATORZE BEZPIECZEŃSTWA INFORMACJI** – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony danych osobowych,
8. **PODMIOCIE** – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nieposiadający osobowości prawnej, jednostkę budżetową.

§ 3. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik nr 1 do Polityki Bezpieczeństwa.**

§ 4. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik nr 2 do Polityki Bezpieczeństwa.**

§ 5. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik nr 3 do Polityki Bezpieczeństwa.**

§ 6. W podmiocie dba się o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty znajdują się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 7. 1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych.

2. Administrator Danych Osobowych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Administrator Danych Osobowych nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **załącznik nr 4 do Polityki Bezpieczeństwa**.
4. Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w podmiocie, a w szczególności:
   1) Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik nr 5 do Polityki Bezpieczeństwa,**
   2) Zestawienie danych osobowych - kiedy i przez kogo zostały do zbioru wprowadzone, oraz komu są przekazywane – **załącznik nr 6 do Polityki Bezpieczeństwa**.
   3) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – **załącznik nr 7 do Polityki Bezpieczeństwa.**

§ 8. Na wniosek osoby, której dane dotyczą, Administrator Danych Osobowych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 9. Administrator Danych Osobowych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Wzór umowy stanowi – **załącznik nr 8 do Polityki Bezpieczeństwa.**

§ 10. Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje **INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**.

§ 11. W celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych wdraża się dokument o nazwie **PROCEDURA ALARMOWA**, stanowiący uzupełnienie Polityki Bezpieczeństwa w podmiocie.

§ 12. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie odpowiednie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. 2014 r., poz. 1182, zm. poz. 1662 oraz z 2015 r. poz. 1309.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024).

§ 13. 1. Administrator Danych Osobowych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.

2. Polityka Bezpieczeństwa określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.
3. Polityka Bezpieczeństwa dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne), oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Celem Polityki Bezpieczeństwa jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.
5. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce Bezpieczeństwa.
6. Cele Polityki Bezpieczeństwa realizowane są poprzez zapewnienie danym osobowym następujących cech:
   1) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
   2) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   3) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
   4) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.
7. Dla skutecznej realizacji Polityki Bezpieczeństwa Administrator Danych Osobowych zapewnia:
   1) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne,
   2) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
   3) kontrolę i nadzór nad przetwarzaniem danych osobowych,
   4) monitorowanie zastosowanych środków ochrony,
   5) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa,
   6) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone,
8. Monitorowanie przez Administratora Danych Osobowych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
9. Administrator Danych Osobowych lub osoba przez niego upoważniona wdraża wszystkie niezbędne dokumenty wynikające z zapisów ustawy, oraz innych przepisów mających zastosowania przy przetwarzaniu danych osobowych.

Administrator Danych Osobowych

…….
(pieczątka, podpis)