Załącznik do zarządzenia Nr 0050.113.2018

Burmistrza Miasta Zambrów z dnia 26 listopada 2018r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

Wstęp

1. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych j z przetwarzaniem danych osobowych iw sprawie swobodnego przepływu takich danych oraz dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).
2. Celem wdrożenia niniejszej dokumentacji jest zapewnienie należytej ochrony danych osobowych będących w zasobach Administratora Danych, w szczególności odpowiedniej do zagrożeń i kategorii danych osobowych objętych ochroną.
3. Poprzez bezpieczeństwo danych osobowych należy rozumieć zapewnienie ich poufności, integralności, dostępności oraz rozliczalności, poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i procedur organizacyjnych.
4. Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie zbiory danych osobowych przetwarzane przez Administratora Danych, zarówno w formie elektronicznej, jak i papierowej oraz dane osobowe przetwarzane poza zbiorami danych.
5. Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników mających dostęp do danych osobowych, przy pomocy, których Administrator Danych wykonuje swoje czynności.
6. Niniejsza Polityka została opracowana w oparciu o standardy PN-ISO/1EC 27001:2014-12, natomiast ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie standardów PN- ISO 27000:2014.

Rozdział 1.
Deklaracja i zastosowanie

§1.1. Realizując obowiązki wynikające z przepisów dotyczących ochrony danych osobowych Administrator Danych dąży do spełnienia wymagań chroniących prywatność i godność interesantów, kontrahentów oraz pracowników Urzędu.

2. Wypełniając Politykę Bezpieczeństwa w zakresie ochrony danych osobowych Urząd Miasta Zambrów dokłada szczególnej staranności w celu zapewnienia bezpieczeństwa przetwarzanych danych oraz zaangażowanie w podejmowanie przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.

3. Dokument - Polityka ochrony danych osobowych w Urzędzie Miasta Zambrów, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia zgodności z prawem, rzetelności i przejrzystości przetwarzania danych, gwarancji adekwatności danych oraz ich minimalizacji, zbierania w konkretnych, wyraźnych i prawnie uzasadnionych celach. Dokument jest jednym ze środków organizacyjnych wprowadzonych przez Administratora Danych, mającym na celu wykazanie rozliczalności ~ przestrzegania przepisów ujętych w art. 5 ust. 1 RODO. Polityka odnosi się do zbiorów przetwarzanych w sposób tradycyjny - manualny oraz za pomocą systemu informatycznego.

4. Pracownicy zobowiązani są przestrzegać zasad bezpieczeństwa danych określonych w Polityce ochrony danych, a także współpracować we wdrażaniu oraz doskonaleniu procedur ochrony danych.

5. Celem opracowania Polityki ochrony danych osobowych jest określenie zasad ochrony danych osobowych przetwarzanych w Urzędzie Miasta Zambrów. Zasady określone w niniejszej Polityce mają zastosowanie do wszystkich osób upoważnionych przez administratora do przetwarzania danych osobowych, osobowych niezależnie od formy ich zatrudnienia. Utrzymanie bezpieczeństwa przetwarzanych przez Urząd danych osobowych oraz informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności oraz rozliczalności na wysokim poziomie.

6. Procedury i dokumenty związane z Polityką będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku.

Rozdział 2.
Definicje

§ 2. Ilekroć w Polityce Ochrony Danych Osobowych jest mowa o:

1) rozporządzeniu (RODO) – rozumie się przez to 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;
2) ustawie – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;
3) dane osobowe - oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4) zbiorze danych - rozumie się przez to każdy uporządkowany zestaw danych osobowych dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
5) szczególnej kategorii danych - oznacza dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
6) dane dotyczące wyroków sądowych i naruszeń prawa - oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;
7) dane dzieci - oznaczają dane osób poniżej 16. roku życia;
8) przetwarzaniu danych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
9) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
10) zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
11) usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która me pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
12) pseudonimizacji - przetworzenie danych osobowych, w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
13) zgoda osoby, której dane dotyczą - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą w formie oświadczenia bądź wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
14) bezpieczeństwie danych - rozumie się przez to zapewnienie poufności, integralności i dostępności informacji, a także takich właściwości jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
15) incydencie – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które zagrażają bezpieczeństwu informacji;
16) Administratorze danych osobowych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 Ustawy o ochronie danych osobowych, decydujący o celach i środkach przetwarzania danych osobowych - Burmistrz Miasta Zambrów;

17) Inspektorze ochrony danych - rozumie się przez to osobę powołaną przez administratora danych osobowych w celu nadzoru nad przestrzeganiem stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
18) podmiocie przetwarzającym - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
19) odbiorcy - oznacza osobę fizyczną bądź prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią;
20) Urzędzie - rozumie się przez to zespół osób i środków zapewniający realizację funkcji organu Gminy Miasta Zambrów – Urząd Miasta Zambrów.

Rozdział 3.
Administrator danych osobowych

§ 3. 1. Administrator danych osobowych stosuje środki techniczne i organizacyjne zapewniające ochronę danvch osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych oraz zabezpiecza posiadane dane przed: ich udostępnieniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem przez osobę nieupoważnioną.

2. Administrator w szczególności zapewnia:

l) środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;

2) system i sprzęt informatyczny umożliwiający bezpieczne przetwarzanie danych;

3) aby do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych;

4) zapoznanie z przepisami o ochronie danych osobowych każdej osoby upoważnionej do przetwarzania danych osobowych;

5) prowadzenie ewidencji osób upoważnionych;

6) należyte i terminowe udzielanie informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji zgodnie z rozporządzeniem (RODO).

Rozdział 4.
Inspektor ochrony danych

§ 4. 1 Administrator danych osobowych wyznacza Inspektora ochrony danych w celu nadzoru nad przestrzeganiem stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

2. Administrator danych osobowych jest zobowiązany zawiadomić o wyznaczeniu Inspektora ochrony danych organ nadzorczy oraz opublikować jego dane kontaktowe.

3. Do zadań Inspektora ochrony danych należy:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia (RODO) oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

2) monitorowanie przestrzegania rozporządzenia (RODO), innych przepisów Unii lub państw członkowskich nie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia (RODO);

4) współpraca z organem nadzorczym Prezesem Urzędu Ochrony Danych Osobowych;

5) uczestniczenie od najwcześniejszego etapu we wszystkich kwestiach związanych z ochroną danych osobowych;

6) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia (RODO) oraz stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

4. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
5. Status inspektora ochrony danych.
1) Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
2) Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 rozporządzenia (RODO), zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej;
3) Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego;
4) Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia;
5) Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań - zgodnie z prawem Unii lub prawem państwa członkowskiego.

Rozdział 5.
Polecenie przetwarzania danych

§ 5.1. Za bezpieczeństwo danych osobowych odpowiedzialny Administrator danych osobowych oraz każda osoba upoważniona przez Burmistrza Miasta Zambrów do przetwarzania danych osobowych, niezależnie od formy zatrudnienia.
2. Zgodnie z wymaganiami rozporządzenia do przetwarzania danych dopuszczone są jedynie osoby upoważnione wyłącznie na polecenie Administratora.
3. Administrator danych osobowych upoważniając osoby do przetwarzania danych osobowych kieruje się zasadami:
1) dostęp do danych osobowych umożliwia się osobie w takim zakresie, w którym jest to niezbędne do realizacji powierzonych zadań;
2) każda z osób upoważnionych do przetwarzania danych osobowych zostanie, przed dopuszczeniem do przetwarzania przeszkolona z wymagań dotyczących ochrony danych osobowych oraz poinformowana o konsekwencjach prawnych jakie jej grożą za naruszenie tych zasad.
4. Reguły zatrudnienia pracownika przy przetwarzaniu danych, etap naboru oraz zakończenia stosunku pracy oraz ogólne zasady bezpieczeństwa osobowego zawarte są w odrębnym dokumencie wprowadzonym Zarządzeniem Burmistrza Miasta Zambrów.
5. Administrator danych osobowych postanawia, że do wydawania upoważnień do przetwarzania danych osobowych upełnomocniony zostaje Inspektor ochrony danych, który czuwa również nad aktualnością przyznawanych upoważnień w związku ze zmianami kadrowymi.
6. Wszystkie upoważnienia do przetwarzania danych znajdują się w ewidencji osób upoważnionych do przetwarzania danych, którą prowadzi Inspektor ochrony danych;
7. Wzór ewidencji osób upoważnionych stanowi załącznik nr 1 do niniejszej Polityki;
8. Osoby nieupoważnione do przetwarzania danych osobowych, mogą przebywać w obszarze przetwarzania oraz przechowywania danych osobowych podczas nieobecności osoby upoważnionej do przetwarzania wyłącznie za zgodą Administratora danych osobowych.

Rozdział 6.
Przetwarzanie danych

§ 6. 1. Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z warunków określonych w art. 6 (rozporządzenia) RODO.

2. Podstawa przetwarzania danych w Urzędzie Miasta Zambrów będzie wynikała przede wszystkim z następujących ustępów art. 6 rozporządzenia (RODO):

1) ust. 1 lit. b) - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

2) ust. 1 lit c) - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na

Administratorze;

3) ust. 1 lit. e) - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

3. W sporadycznych przypadkach Urząd Miasta Zambrów przetwarzanie danych osobowych będzie opierał na podstawie art. 6 ust. 1 lit a) rozporządzenia (RODO) - zgoda osoby, której dane dotyczą lub na podstawie art. 6 ust. 1 lit. d) rozporządzenia (RODO) - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (takie sytuacje najczęściej będą miały miejsce w przypadku realizowania zadań z zakresu zarządzania kryzysowego).

Rozdział 7.

Zasady ochrony danych

§ 7. Zarządzanie bezpieczeństwem ochrony danych osobowych zgodnie z wymaganiami niniejszej polityki opiera się na następujących niezaprzeczalnych zasadach:

1) zasada znajomości wymagań Polityki Ochrony Danych Osobowych - każdy pracownik powinien zostać zapoznany z regułami oraz kompletnymi i aktualnymi procedurami ochrony danych osobowych i podpisać stosowne oświadczenie o zapoznaniu się z zasadami obowiązującej Polityki;
2) zasada uprawnionego dostępu - każdy pracownik stosuje się do obowiązujących zasad ochrony danych osobowych, spełnia kryteria dopuszczenia do przetwarzania;
3) zasada przywilejów koniecznych - każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonania powierzonych mu zadań;
4) zasada wiedzy koniecznej - każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań;
5) zasada usług koniecznych - systemy świadczą tylko te usługi, które są konieczne do realizacji zadań statutowych Urzędu;
6) zasada świadomości zbiorowej - wszyscy pracownicy są świadomi konieczności ochrony danych osobowych, zasobów informacyjnych i aktywnie uczestniczą w tym procesie;
7) zasada indywidualnej odpowiedzialności - za bezpieczeństwo poszczególnych zbiorów danych odpowiadają konkretne osoby;
8) zasada obecności koniecznej - prawo przebywania w określonych miejscach mają tylko osoby do tego upoważnione;
9) zasada stałej gotowości - system jest przygotowany na wszelkie zagrożenia, niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających;
10) zasada najsłabszego ogniwa - poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element. Elementy te są wyznaczane na podstawie analizy ryzyka;
11) zasada kompletności - skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania danych;
12) zasada ewolucji - każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych;
13) zasada adekwatności - używane środki techniczne i organizacyjne winny być odpowiednie do sytuacji;
14) zasada segregacji zadań - zadania i uprawnienia powinny być tak podzielone, aby jedna osoba nie mogła samodzielnie decydować o funkcjonowaniu całego systemu.

§ 8. 1. W celu zwiększenia efektywności ochrony danych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

2. Cele i strategie bezpieczeństwa:

1) zgodność z prawem;

2) ochrona zasobów informacyjnych i innych aktywów;

3) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa danych osobowych, zasobów,

rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań;

4) zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty;

5) zapewnienie odpowiedniego poziomu wiedzy dotyczącej ochrony danych osobowych wśród pracowników i współpracowników poprzez zapewnienie odpowiednich szkoleń.

§ 9. Realizacje zamierzeń określonych w § 8 powinny zagwarantować następujące założenia:

1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych oraz odpowiedzialność za ochronę danych;

2) przeszkolenie pracowników w zakresie ochrony danych;

3) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory);

4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń;

5) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych;

6) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii;

7) okresowe aktualizowanie Polityki ochrony danych osobowych;

8) identyfikacja zagrożeń i analiza ryzyka.

Rozdział 8.
Zdarzenia naruszające ochronę danych

§ 10. 1. Zgodnie z art. 34 rozporządzenia (RODO) Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

2. Opis zdarzeń naruszających ochronę danych osobowych przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych oraz postępowania w przypadku naruszenia ochrony danych znajduje się w Polityce zarządzania ryzykiem utraty bezpieczeństwa danych, wprowadzonej odrębnym zarządzeniem.

Rozdział 9.

Udostępnianie danych osobowych

§ 11. 1. Udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

2. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały ujawnione.

3. Podmiot występujący o ujawnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymywania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku ujawnienie danych jest prawnie dopuszczalne i czy nie będzie stanowić ono naruszenia zasad ochrony danych osobowych *(Motyw 31 RODO)*.

4.Udostępnienie danych może nastąpić jedynie na podstawie pisemnego wniosku strony trzeciej. Wniosek zawierać co najmniej dane wnioskodawcy, dane Administratora Danych (celem potwierdzenia właściwości skierowania wniosku o udostępnienie danych osobowych), podstawę prawną upoważniającą do pozyskania informacji, wskazanie przeznaczenia dla udostępnionych danych, zakres informacji.

Rozdział 10.
Podmiot przetwarzający

§12. 1. W przypadku zawierania umów z firmami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów zarządzania bezpieczeństwem ochrony danych niezbędne jest zawarcie umowy powierzenia przetwarzania danych osobowych i określenie w niej następujących wymagań bezpieczeństwa:

1) zakres i cel czynności oraz danych mających być przedmiotem zawartej umowy;

2) zakres odpowiedzialności w przypadku utraty bądź ujawnienia danych;

3) opis środków technicznych i organizacyjnych niezbędnych w celu zachowania bezpieczeństwa danych osobowych;

4) warunki dostępu do informacji - zobowiązanie do zachowania poufności osób uczestniczących w procesie przetwarzania;

5) wyznaczenie terminu obowiązywania umowy, uwzględniając bezterminowy obowiązek zachowania poufności;

0) wymaganych działań w momencie zakończenia umowy.

2. Inspektor ochrony danych prowadzi Rejestr umów powierzenia przetwarzania danych osobowych, stanowiący załącznik nr 2 do niniejszej Polityki.

Rozdział 11.
Rejestr Czynności przetwarzania

§ 13. 1. Zgodnie z art. 30 rozporządzenia (RODO) Administrator zobowiązany jest prowadzić rejestr czynności przetwarzania, który zawiera:

1) nazwisko lub nazwę oraz dane kontaktowe administratora danych osobowych;

2) dane kontaktowe inspektora ochrony danych;

3) cele przetwarzania;

4) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;

5) kategorie odbiorów, którym dane osobowe zostały lub zostaną ujawnione;

6) jeżeli to możliwe planowane terminy usunięcia poszczególnych danych.

2. Rejestr czynności przetwarzania wprowadzony zostanie odrębnym Zarządzeniem

Burmistrza Miasta

Rozdział 12.
Środki organizacyjne i techniczne

§ 14. 1. Administrator Danych Osobowych jest zobowiązany zastosować środki techniczne i organizacyjne, zapewniające ochronę danych osobowych, adekwatne do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2 Zastosowane środki organizacyjne i techniczne znajdują się w odrębnym dokumencie wprowadzonym Zarządzeniem Burmistrza Zambrów.

Rozdział 13.
Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych

§ 15.1. Analiza jest podstawą podejmowania działań zapobiegawczych i ich priorytetyzacji, a jej posiadanie pozwala szerzej spojrzeć na funkcjonowanie procesu przetwarzania danych w Urzędzie.

2. Dokonując analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych należy zwrócić szczególną uwagę na:

1) zagrożenia występujące podczas przetwarzania danych;

2) aktywa, które mogą zostać zagrożone;

3) prawdopodobieństwo wystąpienia ryzyka, a także ewentualny wpływ zdarzenia na aktywa;

4) wdrożenie odpowiednich środków zaradczych;

5) stosowanie okresowych przeglądów i zmian w analizie, w miarę pojawiania się nowych zagrożeń.

Rozdział 14.
Ocena systemu ochrony danych

§ 16. 1. Inspektor ochrony danych jest zobowiązany do sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania, w tym zakresie nie rzadziej niż raz w roku.

2. Zakres sprawdzenia obejmuje przede wszystkim weryfikację wymagań zawartych w:

1) w rozporządzeniu ogólnym o ochronie danych;

2) w przepisach krajowych dotyczących ochrony danych osobowych;

3. Sprawdzenia dokonuje się poprzez:

1) analizę kompletności oraz zgodności dokumentacji przetwarzania danych;

2) stwierdzenia stanu faktycznego w zakresie przetwarzania danych;

3) zgodności stanu faktycznego z przewidzianymi w dokumentacji środkami organizacyjnymi i technicznymi służącymi przeciwdziałaniu zagrożeniom dla ochrony danych osobowych.

4. Sprawdzenie może być doraźne, planowe lub na żądanie Administratora danych osobowych bądź Prezesa Urzędu Ochrony Danych Osobowych.

5. Inspektor ochrony danych zawiadamia Administratora danych osobowych lub Podmiot przetwarzający o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia na żądanie Prezesa Urzędu Ochrony Danych Osobowych w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

6. Zawiadomienia nie przekazuje się w przypadku:

1) sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce;

2) sprawdzenia, o którego dokonanie zwrócił się Prezes UODO, jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin.

7. Po zakończeniu sprawdzenia Inspektor ochrony danych przygotowuje protokół.

8. Protokół jest sporządzany w postaci elektronicznej albo w postaci papierowej.

Rozdział 15.
Obowiązek informacyjny

§ 17. 1. Administrator danych osobowych jest zobowiązany poinformować osobę, której dane dotyczą o przysługujących jej prawach oraz udzielić informacji - odnośnie przetwarzania jej danych osobowych zgodnie z art. 13 lub 14 rozporządzenia (RODO).

2. Administrator zawiera na wnioskach tworzonych przez Urząd, rozpoczynających daną sprawę klauzulę **dotyczącą** zasad i sposobu przetwarzania danych, zawierającą, w szczególności:

1) dane administratora;

2) dane kontaktowe inspektora ochrony danych;

3) cele przetwarzania danych oraz podstawę prawną;

4) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;

5) okres przez który dane osobowe będą przechowywane;

6) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

7) informację o prawie do cofnięcia zgody na przetwarzanie danych w dowolnym momencie;

8| informację o prawie wniesienia skargi do organu nadzorczego.

3. Klauzule informacyjne dotyczące przetwarzania danych osobowych w Urzędzie Miasta Zambrów udostępnione są na stronie internetowej Urzędu (www.zambrow.pl), w Biuletynie Informacji Publicznej oraz na tablicach ogłoszeń w siedzibie administratora (Urząd Miasta Zambrów, 18-300 Zambrów, ul. Fabryczna 3).

Rozdział 16.
Realizacja praw osób, których dane dotyczą

§ 18. 1. Uwzględniając prawa osób, których dane dotyczą zawarte w art. 15-23 rozporządzenia (RODO), realizacja odbywa się na pisemny wniosek osoby zainteresowanej skierowany bezpośrednio do Administratora bądź do Inspektora ochrony danych.

2. Osobie której dane dotyczą przysługuje prawo do:

1) dostępu do danych osobowych, w tym uzyskaniu kopii;
2) sprostowania danych - w przypadku, gdy i dane osobowe są nieprawidłowe bądź niekompletne na podstawie złożonego wniosku osoby, której dane dotyczą;
3) usunięcia danych, jeżeli:
   a) dane osobowe nie są już niezbędne do celów do, których zostały zebrane,
   b) osoba, której dane dotyczą cofnęła zgodę, na której opiera się przetwarzanie,
   c) dane osobowe, były przetwarzane niezgodnie z prawem,
4) ograniczenia przetwarzania w przypadkach, gdy:
   a) osoba kwestionuje prawidłowość danych osobowych,
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą sprzeciwia się usunięciu danych,
   c) administrator już nie potrzebuje danych osobowych do celów przetwarzania, a są one potrzebne osobie, której dane dotyczą,
   d) osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania danych.
5) prawo do sprzeciwu - osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy powierzonej Administratorowi.

3. Dane osobowe, w których posiadaniu jest Urząd Miasta Zambrów nie będą podlegały zautomatyzowanemu przetwarzaniu i profilowaniu.

Rozdział 17.
Odpowiedzialność karna

§ 19. 1. Niezastosowanie się do prowadzonej przez Administratora danych osobowych Polityki ochrony danych osobowych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące:

1) odpowiedzialnością dyscyplinarną;
2) rozwiązaniem stosunku pracy na podst. art. 52 Kodeksu Pracy;
3) odpowiedzialnością karna wynikająca z krajowych przepisów dotyczących ochrony danych osobowych.

Rozdział 18.
Postanowienia końcowe

§ 20. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

§ 21. Każda osoba, upoważniona do przetwarzania danych osobowych w Urzędzie Miasta Zambrów zobowiązana jest zapoznać się z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

§ 22. Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.

Załącznik Nr l do Polityki ochrony danych

Ewidencja osób upoważnionych do przetwarzania danych osobowych

nr upoważnienia	imię i nazwisko osoby upoważnionej	stanowisko	zakres upoważnienia	program służący do przetwarzania danych oraz login z upoważnienia	data otrzymania upoważnienia	data wygaśnięcia upoważnienia

Rejestr umów powierzenia przetwarzania danych

r **nr umowy**	**data zawarcia umowy**	**nazwa podmiotu przetwarzającego**	**zakres powierzenia** **/kategoria danych**	**okres obowiązywania**