BURMISTRZ OKONKA
ul. Niepodległości 53
64-965 OKONEK

Zarządzenie nr 91/2018

Burmistrza Okonka

z dnia 15 października 2018 r.

w sprawie wprowadzenia Polityki bezpieczeństwa w Urzędzie Miejskim w Okonku.

Na podstawie art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), zarządzam, co następuje:

§1

Wprowadzam Politykę bezpieczeństwa w Urzędzie Miejskim w Okonku, której treść stanowi załącznik do niniejszego zarządzenia.

§2

Zobowiązuję wszystkich pracowników Urzędu Miejskiego w Okonku do zapoznania się i stosowania Polityki bezpieczeństwa.

§3

Wykonanie zarządzenia powierza się Sekretarzowi Miasta i Gminy Okonek.

§4

1. Zarządzenie wchodzi w życie z dniem 15 października 2018.
2. Od dnia wejścia w życie niniejszego Zarządzenia, traci moc Zarządzenie nr 100/2012 Burmistrza Okonka z dnia 6 listopada 2012 r. w sprawie „Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Okonku" i „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych w Urzędzie Miejskim w Okonku".

BURMISTRZ OKONKA
Małgorzata Sameć

POLITYKA BEZPIECZEŃSTWA

w Urzędzie Miejskim w Okonku

Rozdział 1. Postanowienia ogólne

§1. Postanowienia polityki

Niniejszy dokument opisuje reguły dotyczące zapewnienia bezpieczeństwa danych osobowych zawartych w Urzędzie Miejskim w Okonku.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich, którzy przetwarzają dane osobowe w jednostce.

Dokument zwraca uwagę na konsekwencje, jakie mogą wynikać z niewłaściwego przetwarzania danych osobowych oraz procedury postępowania dla zapobiegania i minimalizacji skutków zagrożeń.

Dokument „Polityka bezpieczeństwa przetwarzania danych osobowych" zgodnie z RODO, określa sposób postępowania celem minimalizacji naruszenia bezpieczeństwa przy przetwarzaniu danych osobowych a także sposób postępowania w sytuacji wystąpienia incydentu.

Potrzeba opracowania „Polityki bezpieczeństwa przetwarzania danych osobowych", wynika z przepisów art.24 RODO, który do obowiązków administratora zalicza wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się zgodnie z rozporządzeniem i aby móc to wykazać.

Zasady stosowanych środków powinny uwzględniać charakter, zakres i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa powyżej obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

§2. Przepisy ogólne

1. Celem Polityki bezpieczeństwa jest wdrażanie odpowiednich metod, które spowodują właściwe postępowanie i zabezpieczenie zasobów związanych z przetwarzaniem danych osobowych;
2. Polityka bezpieczeństwa określa tryb i zasady postępowania w przypadku, gdy:
   1) ujawnione zostaną sytuacje wskazujące na wystąpienie incydentu z naruszeniem ochrony danych osobowych,
   2) zostały zanalizowane określone ryzyka naruszenia celem minimalizacji ryzyka;

2. Realizacja zapisów w „Polityce bezpieczeństwa" ma zapewnić właściwą i skuteczną reakcję, ocenę
i dokumentowanie przypadków wystąpienia incydentów;

3. Niniejsza Polityka 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 (ogólne rozporządzenie o ochronie danych - dalej RODO) (Dz.Urz. UE L 119, s. 1),

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

§3. Definicje:

1) „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 (ogólne rozporządzenie o ochronie danych dalej RODO);

2) „ustawa"

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

3) „inspektor ochrony danych"

osoba, podmiot powołany przez administratora danych do realizacji zadań wynikających z RODO celem skutecznej ochrony danych osobowych ;

4) „dane osobowe"

oznaczają 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;

5) „przetwarzanie"

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 przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

6) „incydent"

naruszenie ochrony danych osobowych w sposób zamierzony lub niezamierzony , które może powodować stratę oraz skutki negatywne dla bezpieczeństwa zasobów;

7) „ograniczenie przetwarzania"

oznacza przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

8) „profilowanie"

oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby

fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

9) „pseudonimizacja"

oznacza 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;

10) „zbiór danych"

oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

11) „administrator"

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

12) „podmiot przetwarzający"

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

13) „odbiorca"

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

14) „strona trzecia"

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

15) „zgoda" osoby

której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

16) „naruszenie ochrony danych osobowych"

oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

17) „przedstawiciel"

oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;

18) „przedsiębiorca"

oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;

19) „organ nadzorczy"

oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51;

20) „zgodność przetwarzania danych osobowych „

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

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;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

21) „warunki wyrażenia zgody"

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.

3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

§4. Inspektor Ochrony Danych Osobowych

1. Zadaniem inspektora ochrony danych jest działanie na rzecz zgodnego z prawem przetwarzania danych;
2. Administrator oraz podmiot przetwarzający ma obowiązek właściwego i bezzwłocznego włączania Inspektora we wszystkie sprawy dotyczące ochrony danych osobowych (art. 38 ust. 1 RODO). Administrator danych lub podmiot przetwarzający powinien umożliwić inspektorowi ochrony danych czynny udział we wszystkich sprawach dotyczących procesów przetwarzania danych osobowych oraz na bieżąco przekazywać mu wszystkie informacje związane z wykonywaniem jego zadań. Tym samym wiedza inspektora ma obejmować informacje o każdej sprawie dotyczącej przetwarzania i ochrony danych osobowych, w danej jednostce organizacyjnej;
3. Inspektor ochrony danych, w związku z pełnieniem swojej funkcji, realizuje swoje zadania rzetelnie, a także charakteryzuje się wysokim poziomem etyki zawodowej oraz poprzez priorytetowe traktowanie swoich obowiązków;
4. Inspektor w zakresie swoich obowiązków podlega bezpośrednio administratorowi. Administrator wspiera Inspektora w wypełnianiu jego zadań;
5. Administrator zapewnienia udział Inspektora we wszystkich zagadnieniach związanych z ochroną danych osobowych;
6. Administrator nie powinien wydawać inspektorowi instrukcji co do wykonywania przez niego zadań.

§5. Zadania Inspektora Ochrony Danych

1) informowanie administratora 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 przepisów krajowych, rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych;
3) podejmowanie działań zwiększających świadomość pracowników przetwarzających poprzez szkolenia personelu uczestniczącego w operacjach przetwarzania;
4) prowadzenie okresowych przeglądów stanu zabezpieczenia danych osobowych, audytów i przedstawianie ich wyników administratorowi danych osobowych;
5) realizacja zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
6) współpraca z organem nadzorczym;
7) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
8) w przypadku incydentu związanego z naruszeniem ochrony danych osobowych pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia (RODO);
9) prowadzenie rejestru czynności na zbiorach;
10) prowadzenie dokumentacji dla administratora danych osobowych;
11) prowadzenie spraw związanych z incydentami, w przypadku ich wystąpienia;
12) dokonywanie oceny i szacowania ryzyka celem zastosowania skutecznych metod organizacyjnych i technicznych dla właściwej ochrony danych osobowych u administratora danych osobowych, a w przypadku potrzeby oceny skutków naruszenia ochrony danych osobowych;
13) przygotowywanie do podpisania przez administratora poleceń - upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób poleceń-upoważnionych.

Rozdział 2. Przetwarzanie danych osobowych

§1. Zasady ogólne

1) wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne.;
2) dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane;

3) zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.;
4) zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących;
5) osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem;
6) konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.;
7) dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum.;
8) dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami;
9) aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.;
10) należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe;
11) dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

§2. Upoważnienie do przetwarzania danych osobowych przez pracowników

1) zgodnie z art. 29 RODO - podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego;
2) wzór polecenia - upoważnienia stanowi załącznik nr 1 do Polityki.

§3. Podmiot przetwarzający – umowa powierzenia

1) jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą;
2) podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich

zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian;

3) przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora;
4) podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
5) umowa powierzenia jest podpisana na piśmie lub w formie elektronicznej;
6) wzór umowy powierzenia stanowi załącznik nr 4 do polityki.

§4. Rejestr czynności przetwarzania

1) zgodnie z art. 30 Rozporządzeniem UE w sprawie ochrony danych osobowych, administrator danych prowadzi rejestr czynności przetwarzana danych osobowych. Jest to dokument, który ma pokazywać w szczególności w jakich procesach w organizacji są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczane. Dokument ten będzie musiał zostać udostępniony na każde wezwanie GIODO;
2) celem prowadzenia ww. rejestru jest możliwości pełnienia nadzoru i monitorowania procesów przetwarzania danych osobowych przez organ nadzorczy;
3) rejestr czynności przetwarzania prowadzony przez ADO wg.RODO jest prowadzony wówczas gdy przetwarzanie :

   - może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą;
   - nie ma charakteru sporadycznego;
   - obejmuje szczególne kategorie danych osobowych ;
   - obejmuje dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO.

4) rejestr może być prowadzony w formie pisemnej i/lub elektronicznej;
5) administrator lub podmiot przetwarzający oraz przedstawiciel administratora lub podmiotu przetwarzającego (jeżeli istnieje) mają obowiązek udostępnić rejestr na każde żądanie organu nadzorczego. Organ nadzorczy dokonuje kontroli tych rejestrów w celu monitorowania operacji przetwarzania;
6) rejestr czynności przetwarzania prowadzony przez administratora danych zawiera :

- nazwę i dane kontaktowe administratora danych;
- nazwy współadministratorów – jeżeli istnieją;
- nazwę przedstawiciela;
- dane kontaktowe inspektora jeżeli został powołany,

- kategorie osób, których dane dotyczą /nazwa zbioru/;
- kategorie danych osobowych;
- kategorie odbiorców, którym dane zostały lub zostaną udostępnione;
- cel przetwarzania danych;
- informację o przekazywaniu danych do państwa trzeciego wraz z dokumentacją opisującą zastosowane zabezpieczenia w tym procesie;
- planowany termin usunięcia danych osobowych;
- ogólny opis zastosowanych zabezpieczeń technicznych i organizacyjnych.

Wzór rejestru czynności przetwarzania stanowi załącznik nr 5 polityki.

Rozdział 3. Incydenty

§1. Zgłoszenie incydentu

1) 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 nakłada na administratora danych obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych;
2) zasady zgłaszania naruszenia ochrony danych organowi nadzorczemu określone są w artykule 33 RODO;
3) administrator danych osobowych ma obowiązek zgłoszenia organowi nadzorczemu przypadek naruszenia ochrony danych osobowych w ciągu 72 godzin. Jeżeli zgłoszenie przekazane zostanie po 72 godz. należy wówczas dołączyć wyjaśnienie przyczyn opóźnienia.;
4) zwolnienie z obowiązku zgłoszenia naruszenia, organowi nadzorczemu możliwe jest, jeżeli jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
5) jeżeli naruszenie dotyczy podmiotu przetwarzającego, to podmiot przetwarzający bez zbędnej zwłoki zgłasza je administratorowi danych;
6) jeżeli informacji nie możemy udzielić w tym samym czasie możemy je przekazywać organowi nadzorczemu sukcesywnie bez zbędnej zwłoki;
7) administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania artykułu 33 RODO;
8) administrator prowadzi rejestr incydentów – wzór rejestru stanowi załącznik nr 6 do Polityki.

§2. Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1) jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu;
2) zawiadomienie, jasnym i prostym językiem powinno opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej niżej wymienione informacje:

- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie nie jest wymagane w następujących przypadkach:

1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

2. Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt. 1.

3. Wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, wymienionych wyżej;

Wzór zawiadomienia stanowi załącznik nr 7 do Polityki.

Rozdział 4. Obowiązek informacyjny – zasady
§1. Informacje jakie należy przekazać osobom, których dane dotyczą

1. Motyw 60 preambuły RODO wskazuje nam, że osoba, której dane dotyczą, musi być poinformowana o prowadzeniu operacji przetwarzania i o jego celach. Poza tym administrator powinien podać wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.
2. Dodatkowo należy poinformować o fakcie profilowania oraz o konsekwencjach takiego profilowania. W przypadku zbierania danych od osoby, której dane dotyczą, należy wskazać, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania.

3. W przypadku, gdy zbieramy dane osobowe, od osoby której dane dotyczą zgodnie z art. 13 ust. 1 i 2 RODO powinniśmy poinformować ją o:

a) swojej tożsamości i danych kontaktowych oraz tożsamośći i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;

b) danych kontaktowych inspektora ochrony danych (jeżeli go powołaliśmy);

c) celach przetwarzania, do których mają posłużyć dane osobowe;

d) podstawie prawnej przetwarzania;

f) prawnie uzasadnionym interesie realizowanym przez administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu ADO ;

g) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

h) transferze danych do państwa trzeciego, w tym o:

- zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
- stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony ,
- lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego ,

i) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

j) prawie do:

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

k) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa
się na podstawie zgody na przetwarzanie danych zwykłych lub szczególnej kategorii ;

l) prawie wniesienia skargi do organu nadzorczego;

m) informacji, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania
i jakie są ewentualne konsekwencje niepodania danych;

n) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

§2. Forma spełnienia obowiązku informacyjnego

1. Powyższe informacje administrator danych powinien przekazać w **formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej** oraz jasnym i prostym językiem w szczególności gdy informacje są kierowane do dziecka (art. 12 ust. 1 RODO),
2. Klauzulę informacyjną można opatrzyć też **standardowymi znakami graficznymi**, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania (Art. 12 ust. 7 RODO),
3. Obowiązek informacyjny możemy spełnić **na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie**. Jednak jeżeli w treści obowiązku informacyjnego zastosowano znaki, a są one przedstawione elektronicznie, muszą nadawać się do odczytu maszynowego. Dodatkowo spełnienie obowiązku informacyjnego w stosunku do osób musi być wolne od opłat.

Wzór obowiązku informacyjnego stanowi załącznik nr 8 do polityki.

§3. Prawo do kontroli przez osobę, której dane osobowe są przetwarzane

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dotyczące jej dane osobowe. Jeżeli dane są przez dany podmiot przetwarzane, to może wnioskować o udzielenie następujących informacji:

1) cele przetwarzania;

2) kategorie danych osobowych;

3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

6) informacje o prawie wniesienia skargi do organu nadzorczego;

7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

9) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

§4. Obowiązek ułatwienia kontroli

Administrator ma obowiązek ułatwiania osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22:

1. Prawo dostępu do swoich danych ,
2. Prawo do sprostowania,
3. Prawo do usunięcia,
4. Prawo do ograniczenia,
5. Prawo do przenoszenia,
6. Prawo do sprzeciwu,
7. Prawo do informacji o profilowaniu.

Również w przypadkach przetwarzania niewymagającego identyfikacji, administrator nie może odmawiać podjęcia działań na żądanie osoby chcącej zrealizować prawa przysługujące jej na mocy art. 15–22, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.

§5. Obowiązek informowania - terminy

Terminy na wywiązanie się z tego obowiązku to:

1) bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania- zasadniczo,

2) trzy miesiące – w razie potrzeby ww. termin jednego miesiąca można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań,

3) w terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia,

4) Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

§6. Obowiązek uzasadnienia odrzucenia żądania – pouczenie o prawie skargi

Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o:

1) powodach niepodjęcia działań; oraz

2) możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

§7. Wolność od opłat

Prawo do kontroli jest wolne od opłat jednakże:

jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

1) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo

2) odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

§8. Obowiązki osoby, której dane dotyczą, względem administratora

1) Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą,
2) To, że wątpliwości muszą być uzasadnione, oznacza że administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Administrator nie powinien zatrzymywać danych osobowych wyłącznie w celu reagowania na ewentualne żądania,
3) Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, może zażądać, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

Rozdział 5. Analiza i szacowanie ryzyka

§1.

1. Zgodnie z art.24 RODO na administratora oraz podmiot przetwarzający nałożony został obowiązek zastosowania zabezpieczeń danych osobowych zgodnie z oceną zagrożeń.

2. Obowiązki administratora

1) Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2) Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3) Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

§2. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym

prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

3. Każda organizacja przetwarzająca dane narażona jest na wpływ czynników wewnętrznych oraz zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem:

1) zniszczenia,
2) utracenia,
3) zmodyfikowania,
4) nieuprawnionego ujawnienia,
5) nieuprawnionego dostępu.

4. Ocenę ryzyka w zakresie bezpieczeństwa przetwarzania danych osobowych przeprowadzamy biorąc pod uwagę potencjalnie negatywne skutki (straty) zarówno dla administratora jak i dla osób , których dane dotyczą.

§3. Definicje

1) ryzyko – możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów. Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia". W przypadku ryzyka naruszenia praw i wolności osób, których dane dotyczą, celem będzie ochrona tych praw i wolności,
2) szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 25005:2011),
3) identyfikacja ryzyka - jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę,
4) kryteria akceptacji ryzyka – są to kryteria, które określają dopuszczalność danego ryzyka. Zwykle definiuje się je poprzez wartość progową, np. przy przedziałach ryzyka 0-2, 3-5 oraz 6-8, akceptowalną wartością jest ryzyko tylko w zakresie 0-2,
5) kryteria oceny ryzyka - są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka,
6) podatność - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym,

7) zabezpieczenie - jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa,

8) zagrożenie - jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

9) proces przetwarzania danych osobowych – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.

10) operacja przetwarzania danych osobowych - każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

11) anonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi,

12) pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przeciwieństwie do anonimizacji, której skutkiem jest nieodwracalne uniemożliwienie identyfikacji osoby, pseudonimizacja jest procesem odwracalnym.

§4. Ogólne wymogi bezpieczeństwa

1. Przetwarzanie danych osobowych w Urzędzie Miejskim w Okonku odbywa się w postaci:
   1) elektronicznej (np.: pliki na dysku komputera, w pamięci operacyjnej komputera),
   2) papierowej (wydruki).

Aby zapewnić bezpieczeństwo przetwarzania danych osobowych należy stosować:

1) środki ochrony fizycznej stanowiska komputerowego oraz wydruków przed nieuprawnionym dostępem,
2) środki ochrony technicznej stanowiska komputerowego (np.: hasła dostępu do stacji roboczej, program antywirusowy).

2. Aktywa

1) Przetwarzanie danych osobowych odbywa się w Urzędzie Miejskim w Okonku, ul. Niepodległości 53, 64-965 Okonek,

2) Dane osobowe przetwarzane są przez osoby uprawnione , posiadające upoważnienie wydane przez administratora danych osobowych,
3) Prowadzona jest ewidencja wydanych upoważnień do przetwarzania danych osobowych oraz rejestr osób , które podpisały oświadczenie o zapoznaniu z przepisami,
4) Prowadzony jest rejestr czynności przetwarzania danych osobowych,
5) Rejestr czynności przetwarzania prowadzony przez ADO wg.RODO jest prowadzony wówczas gdy przetwarzanie :

- może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą;
- nie ma charakteru sporadycznego;
- obejmuje szczególne kategorie danych osobowych .

Rejestr czynności przetwarzania stanowi załącznik nr 3 do Polityki.

§5. Ewentualne koszty związane z utratą aktywów

1. Koszty związane z odtworzeniem aktywów,
2. Koszty utraty zaufania do administratora danych osobowych,
3. Koszty związane z utratą:
   - poufności,
   - integralności,
   - dostępności danych ,
4. Możliwość nałożenia kary przez organ nadzorczy,
5. Koszty związane z możliwością nakazania przez organ nadzorczy całkowitego zaprzestania lub czasowego zaprzestania przetwarzania danych osobowych , np. w sytuacji niezastosowania przez administratora odpowiednich środków bezpieczeństwa.

§6. Zagrożenia dla systemu informatycznego

Podstawowe zagrożenia dla systemu informatycznego, przeznaczonego do przetwarzania danych osobowych:

1. Utrata poufności (pozyskanie danych przez osoby nieupoważnione):
   1) nieuprawniony dostęp do pomieszczenia gdzie znajdują się dane osobowe(wydruki),
   2) nieuprawniony dostęp do stacji roboczej (komputera) gdzie znajdują się dane osobowe (np. poprzez ujawnienie hasła dostępu),
   3) nieuprawnione skopiowanie danych osobowych na inny nośnik,
   4) zgubienie nośnika zawierającego dane osobowe,
   5) niedostateczne zniszczenie wydruku zawierającego dane osobowe,
   6) klęska żywiołowa powodująca utratę poufności danych.
2. Utrata integralności (zmiany w systemie informatycznym przeprowadzone przez osoby nieupoważnione):
   1) nielegalny dostęp do dokumentów zawierających dane osobowe (w formie papierowej i elektronicznej),
   2) błędy ludzkie,
   3) działania wirusów (brak programów antywirusowych i firewalli),
   4) awarie oprogramowania komputerów,

3. Utrata rozliczalności (brak możliwości przypisania danemu podmiotowi konkretnych działań) :
   1) brak mechanizmu uniemożliwiającego usunięcie logów o pracy danej osoby na komputerze,
   2) brak kontroli nad kopiowaniem dokumentów z komputera na nośniki zewnętrzne.

Do głównych źródeł zagrożeń dla stanowisk komputerowych, na których przetwarzane są dane osobowe przedstawia poniższa tabela:

ŹRÓDŁO ZAGROŻENIA		SPOSÓB ZABEZPIECZENIA
Siły wyższe – naturalne -niezależne od jednostki ludzkiej	• pożar np.: będący skutkiem uderzenia pioruna, • starzenie się sprzętu, • powódź, • katastrofa budowlana, • wilgoć, kurz,	Skutki zagrożeń wynikających z sił natury można starać się ograniczyć poprzez odpowiednia zabezpieczenie budynku, w którym znajdują się dane osobowe.
Działalność człowieka	• błędy użytkowników. • zgubienie nośnika informacji, • niewłaściwe usunięcie danych z nośnika informacji, • terroryzm, • utrata prądu, • szpiegostwo, • kradzież, • wandalizm, • podsłuch, • ataki socjotechniczne.	Zagrożenia wynikające z działalności człowieka mogą zostać ograniczone poprzez rygorystyczne przestrzeganie zasad ochrony danych osobowych obowiązujących oraz systematyczne szkolenia użytkowników.

§7. Analiza zagrożeń i ryzyka

1. Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie go zlikwidować.
2. Zagrożenia i ryzyka w zakresie ochrony danych osobowych:
   - Niedostateczne kwalifikacje Inspektora (w tym brak podnoszenia kwalifikacji),
   - Brak procedur ochrony danych osobowych,
   - Niezgodne z wymogami prawnymi, nieaktualne, nieadekwatne do zagrożeń procedury ochrony danych osobowych,
   - Brak aktualnego wykazu zbiorów będących w zasobach jednostki,
   - Brak lub wady upoważnień do przetwarzania danych osobowych,
   - Udzielanie upoważnienia do przetwarzania danych osobowych osobom postępującym nieetycznie,

- Brak lub wady ewidencji wydanych upoważnień,
- Brak lub wady szkoleń z zakresu ochrony danych osobowych,
- Wady nadzoru nad przetwarzaniem i ochroną danych osobowych,
- Brak lub wady identyfikacji i analizy ryzyka w zakresie przetwarzania i ochrony danych osobowych,
- Brak reakcji lub nieprawidłowa reakcja na zagrożenie bezpieczeństwa danych osobowych lub systemów i sieci teleinformatycznych.

§8. Pojęcie i cele ryzyka

1. Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia". Rozporządzenie w Artykule 32 definiuje cele w zakresie bezpieczeństwa przetwarzania i są to:
   - pseudonimizacja i szyfrowanie danych osobowych,
   - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   - regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. W związku z powyższym ryzyko w przetwarzaniu danych jest związane z potencjalną sytuacją, w której określone zagrożenie wykorzysta podatność (np. niezabezpieczony hasłem sprzęt komputerowy), powodując w ten sposób szkodę dla jednostki organizacyjnej (np. kradzież lub upublicznienie informacji).

§9. Identyfikacja ryzyka (zagrożeń i podatności)

1. Zgodnie z zapisem 75 punktu preambuły Rozporządzenia, wyszczególnione zostały zagrożenia związane z przetwarzaniem danych z wyszczególnieniem prowadzących do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:
   - jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną,
   - jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
   - jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa,

- jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,
- lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci,
- jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

§10. Pomiar i analiza ryzyka

1. Prawdopodobieństwo w terminologii zarządzania ryzykiem to możliwość wystąpienia jakiegoś zdarzenia (np. jako prawdopodobieństwo lub częstość w określonym przedziale czasu).

Zdefiniowanie poziomu ryzyka realizujemy wykorzystując macierz ryzyka , która daje możliwość zobrazowania poziomu zagrożeń.

PRAWDOPODOBIEŃSTWO /RYZYKO/	NISKI	**1-20**
	ŚREDNI	**21-60**
	WYSOKI	**61-80**
	KRYTYCZNY	**81-100**

POZIOM RYZYKA	SPOSÓB DZIAŁANIA
N - niski	**Poziom ryzyka akceptowany** Działania podejmowane są w zależności od wymaganych nakładów
Ś - średni	**Poziom ryzyka nieakceptowany** Działanie może zostać przesunięte w czasie , lecz wymagany jest okresowy nadzór i monitorowanie
W – wysoki	**Poziom ryzyka nieakceptowany** Działanie może zostać przesunięte w czasie , lecz wymagany jest stały nadzór i monitorowanie
K – krytyczny	**Poziom ryzyka nieakceptowany** Wymagana jest niezwłoczna reakcja i działanie

2. Ryzyko szczątkowe – ryzyko, które pozostaje po wprowadzeniu zabezpieczeń, często zwane również ryzykiem pozostałym lub ryzykiem akceptowalnym.

Po analizie zagrożeń i podatności wszystkich czynników występujących czy też mogących wystąpić opisanych dotychczas, niewątpliwie istnieje jeszcze pewne ryzyko dla bezpieczeństwa przetwarzania danych osobowych. W celu bardziej przejrzystego zidentyfikowania pozostałego ryzyka niżej przedstawiono proces analizy ryzyka w oparciu o podaną macierz. W rzędach macierzy wyszczególnione są zasoby podlegające ochronie.

Analiza dotyczy ryzyka jakie zagrażają:

- INTEGRALNOŚCI,
- POUFNOŚCI ,
- DOSTĘPNOŚCI.

INTEGRALNOŚĆ	właściwość zapewniająca, że informacje nie zostały zmienione lub zniszczone w sposób nieautoryzowany – **pożar, katastrofa budowlana, błąd ludzki przy przetwarzaniu danych osobowych, zniszczenie płyty zawierającej jedyną kopię danych osobowych.**
POUFNOŚĆ	właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom – **nieuprawniony dostęp klientów do danych osobowych, zagubienie wydruku .**
DOSTĘPNOŚĆ	właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot .

Skutek	rezultat niepożądanego incydentu, następstwa zaistnienia zagrożeń, szkody mierzone wysokością strat, jakie poniosłaby jednostka organizacyjna w wyniku ujawnienia, utraty lub modyfikacji informacji lub zasobu systemu.
Podatność	słabość zasobów, która może być wykorzystana przez zagrożenie – charakteryzuje łatwość, z jaką dane zagrożenie może wyrządzić szkodę.
Ryzyko	prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobów, aby spowodować ich straty lub zniszczenie.

RYZYKO (iloczyn) : **PODATNOŚĆ X SKUTEK = RYZYKO**

3. Przyjęte wartości związane z oceną zagrożenia:

- **1 - 3** - nie ma realnej szansy wystąpienia zidentyfikowanego zagrożenia; zagrożenie nigdy nie wystąpiło,
- **4 - 7** - zagrożenie jest mało realne, jednak zagrożenie może się pojawić,
- **8 - 9**- zagrożenie jest realne i może pojawić się w nieoczekiwanym momencie, pomimo iż nie wystąpiło w okresie ostatnich 24 miesięcy,
- **10** - zagrożenie jest realne lub bardzo realne; zagrożenie wystąpiło w okresie ostatnich 24 miesięcy.

4. Szacowanie ryzyka integralności

W analizie ustalono cztery poziomy zagrożeń dotyczących zachowania integralności oraz zakres wartości liczbowych (1-10) dla tych poziomów:

Poziomy zagrożeń zachowania INTEGRALNOŚCI informacji	**Zakres wartości liczbowych skutków utraty integralności odpowiadający danemu poziomowi zagrożeń**
Niskie - **N**	1-3
Średnie- **Ś**	4-7
Wysokie - **W**	8-9
Krytyczny – **K**	10

MACIERZ OSZACOWANIA „RYZYKA INTEGRALNOŚCI"

ZASOBY (miejsce)	**SZACOWANIE**	**ZAGROŻENIA**							
		Nielegalny dostęp	Błędy, pomyłki	Celowe uszkodzenia	Nielegalne oprogramowanie	Wirusy	Personel	Awarie	Klęski żywiołowe
Nośniki informacji	SKUTKI	8	6	8	6	5	4	5	4
	PODATNOŚĆ	3	5	3	3	5	6	5	3
	RYZYKO	**24**	**30**	**24**	**24**	**25**	**24**	**25**	**12**
Zgromadzone dane – zbiory	SKUTKI	4	5	6	6	6	5	6	5
	PODATNOŚĆ	6	5	4	4	5	6	5	4
	RYZYKO	**24**	**25**	**24**	**24**	**30**	**30**	**30**	**20**
Oprogramowanie	SKUTKI	6	5	7	5	6	7	6	4
	PODATNOŚĆ	5	6	4	6	7	7	6	5
	RYZYKO	**30**	**30**	**28**	**30**	**42**	**49**	**36**	**20**
Sprzęt komputerowy	SKUTKI	6	6	5	6	6	7	6	4
	PODATNOŚĆ	6	5	4	5	6	7	5	4
	RYZYKO	**36**	**30**	**20**	**30**	**36**	**49**	**30**	**16**

Oszacowanie ryzyka integralności.

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów w ujęciu integralności, informacji . Zgodnie z przyjętą metodyką szacowania ryzyka **poziom wielkości ryzyka** dla obliczonych wartości liczbowych wynosi:

NISKI	**1-20**
ŚREDNI	**21-60**
WYSOKI	**61-80**
KRYTYCZNY	**81-100**

Analizując otrzymane wyniki należy stwierdzić, że nie zanotowano poziomu ryzyka wysokiego i krytycznego.

5. Szacowanie ryzyka poufności

W analizie szacowania ryzyka przyjęto cztery poziomy zagrożeń zachowania „poufności" i 10-cio stopniową skalę skutków utraty „poufności":

Poziomy zagrożeń zachowania POUFNOŚCI informacji	**Zakres wartości liczbowych skutków utraty POUFNOŚCI odpowiadający danemu poziomowi zagrożeń**
Niskie –**N**	1-3
Średnie- **Ś**	4-7
Wysokie- **W**	8-9
Krytyczny –**K**	10

MACIERZ OSZACOWANIA „RYZYKA POUFNOŚCI"

ZASOBY (miejsce)	**SZACOWANIE**	**ZAGROŻENIA**									
		Nielegalny dostęp	Błędy, pomyłki	Pokonanie i omijanie zabezpieczeń	Nielegalne kopiowanie	Nieuprawnione naprawy	Rotacja personelu	Awarie	Klęski żywiołowe	Podsłuch i podgląd	Niedyskrecja
Nośniki informacji	SKUTKI	9	6	6	8	6	5	4	4	5	9
	PODATNOŚĆ	3	5	6	7	7	7	4	4	5	6
	RYZYKO	**27**	**30**	**36**	**56**	**42**	**35**	**16**	**16**	**25**	**54**
	SKUTKI	8	8	8	7	8	6	6	3	7	8

Zgromadzone dane	PODATNOŚĆ	6	5	7	6	5	4	5	3	3	5
	RYZYKO	**48**	**40**	**56**	**42**	**40**	**24**	**30**	**9**	**21**	**40**
Oprogramowanie	SKUTKI	8	8	9	9	7	5	5	4	6	6
	PODATNOŚĆ	3	6	6	5	3	4	4	4	4	4
	RYZYKO	**24**	**56**	**54**	**45**	**21**	**20**	**20**	**16**	**24**	**24**
Sprzęt komputerowy	SKUTKI	8	7	8	2	8	4	6	4	6	6
	PODATNOŚĆ	7	7	7	3	7	5	7	3	6	4
	RYZYKO	**56**	**49**	**56**	**6**	**56**	**20**	**42**	**12**	**36**	**24**

Oszacowanie ryzyka poufności

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów w ujęciu integralności, poufności i dostępności informacji . Zgodnie z przyjętą metodyką szacowania ryzyka **poziom wielkości ryzyka** dla obliczonych wartości liczbowych wynosi:

NISKI	**1-20**
ŚREDNI	**21-60**
WYSOKI	**61-80**
KRYTYCZNY	**81-100**

Analizując otrzymane wyniki należy stwierdzić, że nie zanotowano poziomu ryzyka wysokiego i krytycznego.

6. Szacowanie ryzyka dostępności

W analizie „ryzyka dostępności" przyjęto cztery poziomy zagrożeń zachowania „dostępności" i 10-cio stopniową skalę skutków utraty „dostępności":

Poziomy zagrożeń zachowania „dostępności" informacji	**Zakres wartości liczbowych skutków utraty „dostępności" odpowiadający danemu poziomowi zagrożeń**
Niskie – **N**	1-3
Średnie – **Ś**	4-7
Wysokie – **W**	8-9
Krytycznego – **K**	10

MACIERZ OSZACOWANIA „RYZYKA DOSTĘPNOŚCI"

ZASOBY (miejsce)	SZACOWANIE	ZAGROŻENIA						
		Błędy, pomyłki	Celowe uszkodzenia	Nielegalne oprogramowanie	Infekcja wirusowa	Rotacja personelu	Awarie	Klęski żywiołowe
Nośniki informacji	SKUTKI	2	2	3	3	3	3	4
	PODATNOŚĆ	2	1	2	3	3	3	4
	RYZYKO	**4**	**2**	**6**	**9**	**9**	**9**	**16**
Zgromadzone dane	SKUTKI	6	6	6	6	6	6	6
	PODATNOŚĆ	7	3	3	5	2	2	2
	RYZYKO	**42**	**18**	**18**	**30**	**12**	**12**	**12**
Oprogramowanie	SKUTKI	3	4	2	2	3	3	2
	PODATNOŚĆ	2	3	2	3	2	3	4
	RYZYKO	**6**	**12**	**4**	**6**	**6**	**9**	**8**
Sprzęt komputerowy	SKUTKI	3	4	2	2	3	5	3
	PODATNOŚĆ	4	2	3	3	3	5	2
	RYZYKO	**12**	**8**	**6**	**6**	**9**	**25**	**6**

Oszacowanie ryzyka dostępności

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów i dostępności informacji . Zgodnie z przyjętą metodyką szacowania ryzyka **poziom wielkości ryzyka** dla obliczonych wartości liczbowych wynosi:

Niski	**1-20**
Średni	**21-60**
Wysoki	**61-80**
Krytyczny	**81-100**

Analizując otrzymane wyniki szacowania ryzyka w zakresie integralności, poufności i dostępności należy stwierdzić, że zanotowano średni poziom zagrożeń, natomiast nie zanotowano poziomu ryzyka wysokiego i krytycznego.
Wyniki ryzyka związanego z Bezpieczeństwem Informacji w Urzędzie Miejskim w Okonku są na poziomie nieakceptowanym – średnim.

Ponadto dla skutecznej realizacji zadań związanych z minimalizacją ryzyka należy zwracać szczególną uwagę na:

1) Sprzęt:
   a) Nieuprawnione kopiowanie danych z dysku twardego,
   b) Korzystanie z oprogramowań nie posiadających licencji,
   c) Uszkodzenie sprzętu komputerowego (drukarka, karta sieciowa, jednostka centralna, klawiatura, mysz itp.) oraz łączy transmisyjnych,
   d) Uszkodzenie fizyczne nośników danych,
   e) Starzenie się nośników,
   f) Wejście do systemu operacyjnego z wykorzystaniem obcego identyfikatora.

Nieuprawniony dostęp do procesu przetwarzania danych :

   a) Włamanie do pomieszczeń po godzinach pracy.

2) Ludzie:
   a) Kradzież dokumentów papierowych lub elektronicznych przechowywanych na stanowiskach pracy,
   b) Kradzież dysku twardego komputera,
   c) Zagubienie dokumentów lub utrata w czasie awarii , pożaru, zalania itp.,
   d) Zagubienie dokumentów lub utrata przetwarzanych danych osobowych,
   e) Stosowanie korupcji , szantażu w celu wydobycia określonych informacji od pracowników jednostki,
   f) Infiltracja środowiska przez wyszukiwanie osób uważających się za pokrzywdzonych przez pracodawcę, zwalnianych lub poszukujących zatrudnienia w innej komórce,
   g) Podglądanie zawartości danych znajdujących się na ekranie monitora,
   h) Włamanie do systemu – podszycie się pod uprawnionego użytkownika,
   i) Wyłudzenie , fałszowanie dokumentów, kart dostępu , haseł dostępu itp.,
   j) Nieuprawniona świadoma modyfikacja oprogramowania zainstalowanego na komputerze przez innych użytkowników,
   k) Skorzystanie z cudzego identyfikatora i hasła,
   l) Błędy popełniane przez użytkowników,
   m) Wejście osoby nieupoważnionej do strefy przetwarzania danych osobowych,
   n) Utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych , konserwacji sprzętu ,
   o) Odczytanie danych z nośników przewidzianych do naprawy,
   p) Podgląd danych przetwarzanych przez poprzedniego użytkownika,
   q) Zapisywanie danych na prywatne nośniki użytkownika,
   r) Nieuprawnione kopiowanie danych,

s) Przeglądanie (przeszukiwanie) pamięci operacyjnej i zewnętrznej komputerów w celu uzyskania określonych informacji,
t) Pozostawienie przez pracownika dokumentów , nośników informacji na biurku po godzinach pracy,
u) Utrata kluczowych pracowników,
v) Brak możliwości rozliczania działań użytkowników – brak kontroli nad dostępem do przetwarzanych danych osobowych,
w) Dostęp do informacji przez osoby nieuprawnione podczas ponownego wykorzystania używanych nośników danych,
x) Obserwacja bezpośrednia poprze filmowanie, fotografowanie, nagrywanie.

3) Aplikacje:
a) Nieuprawnione instalowanie urządzeń służących do naruszenia poufności przetwarzanych informacji,
b) Nieuprawniona, świadoma modyfikacja oprogramowania zainstalowanego na komputerze przez innych użytkowników,
c) Korzystanie z nielicencjonowanego oprogramowania,
d) Przypadkowa zmiana ustawień konfiguracyjnych ,
e) Stosowanie niewłaściwego systemu plików,
f) Wykorzystanie przechowywanych dokumentów na dysku twardym.

4) Pomieszczenia:
a) Katastrofy budowlane,
b) Ekstremalne czynniki środowiskowe (temperatura, wilgotność, zapylenie),
c) Awaria klimatyzacji,
d) Pożar w pomieszczeniach, w których są przetwarzane dane osobowe,
e) Zalanie pomieszczeń, w których są przetwarzane dane osobowe,
f) Zamach terrorystyczny.

5) Dodatkowe inne niebezpieczeństwa:
a) Celowe lub przypadkowe zniszczenie zbiorów i programów zewnętrznym impulsem elektromagnetycznym;
b) Podsłuch emisji akustycznych na zewnątrz budynku z obszaru przetwarzania danych osobowych;
c) Awaria zasilania;
d) Awaria systemu operacyjnego lub ujawnienie wady oprogramowania aplikacyjnego;
e) Zbieranie się ładunków elektrostatycznych;
f) Nierzetelna kontrola rejestrowanych zdarzeń systemowych;
g) Wykorzystanie błędów w obiegu dokumentów;
h) Ponowne wykorzystywanie nośników , które powinny być wcześniej skutecznie zniszczone ;
i) Nieprawidłowości w przypadku kserowania , powielania – brak nadzoru lub uprawnień;
j) Niepełny, niedokładny opis procedur w instrukcjach bezpiecznej eksploatacji.

6) Przetwarzanie zautomatyzowane. W odniesieniu do zautomatyzowanego przetwarzania należy wdrożyć po ocenie ryzyka środki, które:
   a) uniemożliwią osobom nieuprawnionym dostęp do sprzętu używanego do przetwarzania (kontrola dostępu do sprzętu);
   b) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);
   c) zapobiegną nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);
   d) zapobiegną korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);
   e) zapewniają, że osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania będą mieć dostęp wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem (kontrola dostępu do danych);
   f) pozwolą zweryfikować i ustalić podmioty, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione za pomocą sprzętu do przesyłu danych (kontrola przesyłu danych);
   g) pozwolą następczo zweryfikować i stwierdzić, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania, kiedy i przez kogo (kontrola wprowadzania danych);
   h) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (kontrola transportu);
   i) zapewniają, że w razie awarii można będzie przywrócić zainstalowane systemy (odzyskiwanie);
   j) zapewniają działanie funkcji systemu, zgłaszanie występujących w nich błędów (niezawodność) oraz odporność przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

Załącznik nr 1

POLECENIE - UPOWAŻNIENIE Nr .../....
do przetwarzania danych osobowych

Na podstawie art. 29 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 dalej RODO) – upoważniam:

.....
(imię i nazwisko pracownika)

.....
(stanowisko służbowe pracownika)

do przetwarzania danych osobowych w zbiorach danych

.....
.....
(wskazać kategorie danych, które może przetwarzać osoba wymieniona w upoważnieniu lub rodzaj czynności lub operacji, jakich może dokonywać na danych osobowych).

Powyższe polecenie-upoważnienie wydaje się na okres od ..... do ..... (stażyści/ praktykanci),

na czas trwania stosunku pracy (pracownicy Urzędu).*

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem, przepisami RODO, oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych i z wewnętrznymi regulacjami Urzędu Miejskiego w Okonku w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu pracy.

Data i podpis upoważniającego

.....

Data i podpis osoby upoważnionej

.....

*niepotrzebne skreślić

Załącznik nr 2

UPOWAŻNIENIE Nr ...

DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 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 dalej RODO)

Upoważniam Panią/Pana.....

zatrudnioną/ego w .....

na stanowisku .....

do samodzielnego przebywania w pomieszczeniach, w których przetwarzane są dane osobowe w Urzędzie Miejskim w Okonku.

Upoważnienie wydaje się na czas trwania zatrudnienia.

Data i podpis upoważniającego

.....

Data i podpis osoby upoważnionej

.....

Załącznik nr 3

Okonek, dnia .....

.....

Imię i nazwisko pracownika

.....

Stanowisko służbowe

Oświadczenie o zobowiązaniu się do zachowania poufności

Oświadczam, że zobowiązuję się zachować w tajemnicy wszelkie informacje o danych osobowych uzyskane w związku z ich przetwarzaniem oraz zobowiązuję się do ich ochrony przed niepowołanym dostępem, a także przestrzegać wszelkich procedur obowiązujących w Urzędzie Miejskim w Okonku dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa.

Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

.....

data i podpis

Załącznik nr 4

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia ..... r. pomiędzy:

Gminą Okonek, z siedzibą w Okonku, adres: ul. Niepodległości 53, 64-965 Okonek, nr NIP: 767-16-57-653, nr REGON: 570791388, reprezentowaną przez ..... Burmistrza Okonka przy kontrasygnacie ..... – Skarbnika Miasta i Gminy

zwaną w dalszej części umowy **„Administratorem"**

a

..... z siedzibą w ....., nr NIP: ....., nr REGON: .....

zwanym w dalszej części umowy **„Podmiotem przetwarzającym"**

§1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 ust. 3 Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) - zwanego w dalszej części „Rozporządzeniem"- dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy głównej następujące dane osobowe ....., znajdujące się w (baza danych) .....
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy (podać nr i nazwę umowy głównej) .....

§3

Prawa i obowiązki administratora

1. Administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania przez niego danych osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami prawa, w tym wymogami Rozporządzenia.
2. Administrator, zgodnie z art. 28 ust. 3 lit. h Rozporządzenia, ma prawo przeprowadzania u Podmiotu Przetwarzającego audytów i kontroli, w celu weryfikacji, czy środki zastosowane przez niego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych, spełniają postanowienia niniejszej Umowy.
3. Administrator ma prawo żądania niezwłocznego, to jest w terminie 7 dni/dnia udostępnienia przez Podmiot Przetwarzający aktualnego rejestru kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w § 4 ust. 2 niniejszej umowy.

§4

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający prowadzi w formie pisemnej oraz elektronicznej rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, stosownie do postanowień przepisu art. 30 ust. 2 Rozporządzenia.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy powierzonych danych, o której mowa w art. 28 ust. 3 lit b Rozporządzenia, przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa lub zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych zgłasza je administratorowi bezzwłocznie, nie później jednak niż w ciągu 36 godzin od stwierdzenia naruszenia.

§5

Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 lit. h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator zobowiązany jest poinformować Podmiot Przetwarzający o terminie i zakresie planowanej kontroli, co najmniej na 7 dni przed jej rozpoczęciem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§6

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Podmiot, któremu Podmiot przetwarzający powierzył przetwarzanie danych osobowych powinien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom Rozporządzenia.
3. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§7

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych,

o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§8

Czas trwania i rozwiązanie umowy

1. Niniejsza umowa zostaje zawarta na czas trwania umowy głównej i ulega rozwiązaniu z chwilą rozwiązania umowy głównej.
2. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. Wszelkie zmiany treści niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
4. Spory mogące wyniknąć przy realizacji umowy będą rozstrzygane przez sąd właściwy dla siedziby Pozwanego.

Administrator	Podmiot przetwarzający

Załącznik nr 5

Rejestr czynności przetwarzania w Urzędzie Miejskim w Okonku – wydział organizacyjny

Administrator danych: Gmina Okonek reprezentowana przez Burmistrza Okonka z siedzibą w Okonku przy ul. Niepodległości 53, 64-965 Okonek. Regon 570791388.

Inspektor ochrony danych: Weronika Kończak, e-mail kadry@okonek.pl

Podstawa prawna prowadzenia zbioru danych art. 30 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 (ogólne rozporządzenie o ochronie danych, dalej RODO):

L. p.	Nazwa czynności przetwarzania	Cel przetwarzania	Kategorie osób i przetwarzanych danych osobowych	Planowany termin usunięcia kategorii danych	Kategorie odbiorców (innych niż podmiot przetwarzający)	Informacja o przekazywaniu danych do państwa trzeciego	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							

Załącznik nr 6

Rejestr incydentów - naruszeń

Data naruszenia/zgłoszenia .....

Godz.: .....

Ilość osób, których dotyczy naruszenie : .....

Zgłoszenie do UODO: ☐ tak ☐ nie

Data zgłoszenia do UODO: .....

Godz. zgłoszenia do UODO: .....

Kategorie danych osób , których naruszenie dotyczy ☐ dane zwykłe,

☐ dane podlegające szczególnej ochronie:

Proponowane środki zabezpieczeń : *np. uzupełnienie – zakup sprzętu IT, szkolenie pracowników.*

Zastosowane środki zabezpieczeń : *np. uniemożliwiono dostęp osobom nieupoważnionym.*

Sposób naruszenia: *np. włamanie.*

Konsekwencje – straty: *np. ujawnione zostały dane osobowe, adres i miejsce zamieszkania .*

Zawiadomienie osób, których dane dotyczą

Nie zawiadomiono, gdyż:

☐ ADO wdrożył odpowiednie środki techniczne i organizacyjne,

☐ ADO zastosował działania mające na celu wyeliminowanie ryzyka naruszenia praw i wolności osób,

☐ Zawiadomienie wymagałoby niewspółmiernych środków.

Zawiadomiono poprzez:

☐ Wysłano pismo ze szczegółowym wyjaśnieniem,

☐ Opublikowano komunikat w środkach masowego przekazu (BIP, gazeta, radio itp.).

INSPEKTOR :

Imię:.....

Nazwisko: .....

Podpis: .....

Załącznik nr 7

Zawiadomienie o naruszeniu ochrony danych osobowych

Dane i adres odbiorcy zawiadomienia

.....

.....

Data naruszenia: .....

Godz. naruszenia: .....

Kategoria osób, których naruszenie dotyczy:

- *np. dane z ewidencji ludności i dowodów osobistych* ,

Rodzaj naruszenia:

- *np. niekontrolowany wypływ poprzez sieć TI.*

Zastosowane środki zabezpieczające:

- *np. wdrożono dodatkowe środki techniczne i organizacyjne w tym: zabezpieczenie w dodatkowe programy antywirusowe, przeszkolono osoby przetwarzające dane osobowe*

Konsekwencje naruszenia:

- *np. ujawnienie danych osobowych i adresów , miejsca zamieszkania oraz numeru nieruchomości.*

Czy zgłoszono incydent do UODO:

- *np. incydent został zgłoszony do Urzędu Ochrony danych osobowych w ciągu 72 godzin od dnia stwierdzenia naruszenia ochrony danych osobowych.*

INSPEKTOR :

Imię : .....

Nazwisko: .....

Nr Tel: .....

e-mail : .....

Załącznik nr 8

Informacja o prywatności

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia 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 (ogólne rozporządzenie o ochronie danych, dalej RODO) informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest Gmina Okonek, reprezentowana przez Burmistrza Okonka z siedzibą w Okonku przy ul. Niepodległości 53, 64-965 Okonek, tel. 67 266 90 03, mail: ratusz@okonek.pl.
2. W sprawach związanych z danymi osobowymi można kontaktować się z inspektorem ochrony danych w Urzędzie Miejskim w Okonku pod adresem: kadry@okonek.pl.
3. Pani/Pana dane osobowe przetwarzane będą w celu wypełnienia obowiązku prawnego ciążącego na Administratorze, na podstawie art. 6 ust. 1 lit. c RODO, bądź wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi, na podstawie art. 6 ust. 1 lit. e RODO.
4. W związku z przetwarzaniem danych w celu wskazanym powyżej, Pani/Pana dane osobowe mogą być udostępniane innym odbiorcom lub kategoriom odbiorców danych osobowych, którymi mogą być:
    1. podmioty upoważnione do odbioru Pani/Pana danych osobowych na podstawie odpowiednich przepisów prawa;
    2. podmioty, które przetwarzają Pani/Pana dane osobowe w imieniu Administratora na podstawie zawartej umowy powierzenia przetwarzania danych osobowych (tzw. podmioty przetwarzające).
5. Pani/Pana dane osobowe nie będą przekazywane do państw trzecich.
6. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji wskazanego powyżej celu przetwarzania, w tym również obowiązku archiwizacyjnego wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz na podstawie przepisów szczególnych określających inny okres archiwalny niż w/w ustawa.
7. W związku z przetwarzaniem przez Administratora danych osobowych przysługuje Pani/Panu prawo: dostępu do treści danych, do sprostowania danych, do usunięcia danych, do ograniczenia przetwarzania danych, do przenoszenia danych, do wniesienia sprzeciwu wobec przetwarzania danych. (Uwaga: realizacja powyższych praw musi być zgodna z przepisami prawa, na podstawie których odbywa się przetwarzanie danych oraz RODO, a także m. in. z zasadami wynikającymi z kodeksu postępowania administracyjnego czy archiwizacji).
8. Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych.
9. Podanie przez Panią/Pana danych osobowych jest:
    1. warunkiem prowadzenia sprawy w Urzędzie Miejskim w Okonku i wynika z przepisów prawa;
    2. dobrowolne, jednak niezbędne do załatwienia sprawy w Urzędzie Miejskim w Okonku.
10. Pani/Pana dane nie będą poddawane zautomatyzowanemu podejmowaniu decyzji, w tym również profilowaniu.