ZARZĄDZENIE NR 138/2018
BURMISTRZA MIASTA MIKOŁAJKI
z dnia 28 grudnia 2018 roku

w sprawie wdrożenia Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy Mikołajki

na podstawie art. 24 ust. 2 rozporządzenia parlamentu Europejskiego i rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w zawiązku z przewarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Ur. UE L119, s. 1) zarządzam, co następuje:

§1.

Wdrażam:

a) Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy Mikołajki, która stanowi załącznik nr 1 do niniejszego zarządzenia.
b) Instrukcję zarządzania systemem informatycznym, która stanowi załącznik nr 2 do niniejszego zarządzania.

§2.

1. Zobowiązuję pracowników do zapoznania się z „Polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy Mikołajki" oraz „Instrukcji zarządzania systemem informatycznym" w terminie 7 dni od wejścia w życie niniejszego zarządzenia.
2. Zobowiązuję pracowników do przestrzegania i stosowania zasad określonych w „Polityce bezpieczeństwa przetwarzania danych osobowych" oraz „Instrukcji zarządzania systemem informatycznym" w Urzędzie Miasta i Gminy Mikołajki.

§3.

Wykonanie zarządzenia powierzam Inspektorowi Ochrony Danych.

§4.

Traci moc Zarządzenie nr 129/2015 z dnia 31.12.2015 r. w sprawie w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych oraz instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy w Mikołajkach.

§5.

Zarządzenie wchodzi z dniem podpisania.

Burmistrz Miasta Mikołajki

Piotr Jakubowski

Załącznik nr 1 do Zarządzenia Burmistrza Miasta Mikołajki nr 138/2018 w sprawie wdrożenia Polityki Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Mikołajkach

<table>
<tr><th colspan="4">POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH</th></tr>
<tr><td colspan="2">URZĄD MIASTA I GMINY W MIKOŁAJKACH ul.
Kolejowa 7
11-730 Mikołajki</td><td>Strona/ stron</td><td>1/10</td></tr>
<tr><td colspan="2">Cel dokumentu:
Określenie zbiorów danych osobowych i zasad ich przetwarzania zgodnie z wymogami Ustawy o Ochronie Danych Osobowych</td><td>Wersja
Z dnia</td><td>28.12.2018</td></tr>
<tr><td>Odpowiedzialny:</td><td>Burmistrz</td><td>Stosowanie:</td><td>Wszystkie stanowiska pracy</td></tr>
</table>

1. SPIS TREŚCI

1 INFORMACJE OGÓLNE

Polityka Bezpieczeństwa danych osobowych jest to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji zasobów zawierających dane osobowe.
Politykę stosuje się do danych osobowych niezależnie od formy, zakresu przetwarzania, oraz lokalizacji zbioru. Poza tym sposób postępowania z danymi musi być zgodny z wymogami prawnymi stosowanymi na terenie Państwa Polskiego, a w szczególności z Ustawą o Ochronie Danych Osobowych oraz Ogólnym Rozporządzeniem o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016, dalej jako RODO).
W przedstawionej dokumentacji za Administratora Danych Osobowych (ADO) rozumie się Burmistrza Miasta Mikołajki reprezentującego Gminę Mikołajki .

ADO jest zobowiązany do:

1. wspierania działań mających na celu ochronę danych osobowych, oraz regularną weryfikację stanu bezpieczeństwa systemu,
2. zastosowania środków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
3. prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych,
4. zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

ADO mocą zarządzenia lub w wyniku zawartej umowy z podmiotem zewnętrznym powołuje Inspektora Ochrony Danych(IOD) . Zmiany na stanowisku IOD regulują odrębne zarządzenia osoby reprezentującej Administratora w obszarze ochrony danych osobowych. Do zadań IOD należy w szczególności:

- Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- Zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- Koordynacja procesu analizy ryzyka związanego z przetwarzaniem danych osobowych,
- Informowanie administratora (lub podmiotu przetwarzającego) oraz pracowników, którzy przetwarzają dane osobowe, o spoczywających na nich obowiązkach i doradzanie im w tej sprawie,
- Koordynacja procesu reakcji na incydenty w zakresie bezpieczeństwa informacji,
- Nadzorowanie zasady bezpieczeństwa danych osobowych przetwarzanych w systemach teleinformatycznych i monitorowanie poziomu bezpieczeństwa IT,
- Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami;
- Sprawowanie nadzoru nad dokumentacją ochrony danych osobowych.

Ochrona danych osobowych przetwarzanych w Gminie Mikołajki (zwany dalej Gmina lub ADO) obowiązuje wszystkie osoby (bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy), które mają dostęp do danych osobowych zbieranych, przetwarzanych oraz przechowywanych w budynkach Urzędu w związku z prowadzoną działalnością. Na potrzeby niniejszej polityki za pracownika uznaje się wszystkie te osoby (niezależnie od stosunku zatrudnienia).
Osoby mające dostęp do danych osobowych zobowiązane są do stosowania środków określonych w niniejszej polityce, regulacjach wewnętrznych Administratora , oraz innych aktach prawnych z którymi pracownik został zapoznany. Środki te mogą wiązać pracownika zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

2 PODSTAWA PRAWNA

Podstawą do opracowania niniejszego dokumentu i jego wdrożenia są następujące przepisy prawa:

a) Konstytucja Rzeczypospolitej Polskiej,
b) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000),
c) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)
d) RODO- Rozporządzenie 2016/679 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.

3 UŻYTE DEFINICJE

1) **Ustawa** - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
2) **Rozporządzenie** - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych
3) **RODO** - Rozporządzenie 2016/679 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
4) **Dane osobowe** – przez dane osobowe rozumie się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. *[def. ustawowa]*
5) **Zbiór danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
6) **Przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych. *[def. ustawowa]*
7) **System informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. *[def. ustawowa]*
8) **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. *[def. ustawowa]*
9) **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych osoby, która składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. *[def. ustawowa]*
10) **Administrator Danych Osobowych (ADO)** – 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. *[def. ustawowa]*
11) **Administrator Systemu Informatycznego (ASI)** – osoba lub dział zajmujący się w szczególności nadzorowaniem pracy serwerów, zarządzaniem kontami użytkowników, konfiguracją komputerów, instalowaniem oprogramowania, dbaniem o bezpieczeństwo systemu i opcjonalnie samych danych, nadzorowanie, wykrywanie i eliminowanie

nieprawidłowości, asystowaniem i współpracą z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych oraz innych zadań wynikających z zaleconych obowiązków.

12) **Inspektor Ochrony Danych (IOD)** - osoba koordynująca z upoważnienia ADO przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.
13) **Odbiorca danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a. osoby, której dane dotyczą,
b. osoby upoważnionej do przetwarzania danych,
c. przedstawiciela w Rzeczypospolitej Polskiej, w przypadku opisanym w art. 31a ustawy o ochronie danych osobowych,
d. podmiotu, któremu w drodze umowy zawartej na piśmie, powierzono przetwarzanie danych,
e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępnione w związku z prowadzonym postępowaniem. *[def. ustawowa]*

14) **Użytkownik systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych zarejestrowaną w systemie informatycznym ADO,
15) **Użytkownik** – należy przez to rozumieć każdą osobę korzystającą z komputera lub urządzenia mobilnego w obszarze bezpiecznym,
16) **Sieć lokalna** – należy przez to rozumieć połączenie systemów informatycznych ADO wyłącznie dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
17) **Sieć publiczna** – należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2017r., poz. 1907) ,
18) **Użytkownik zdalny** - użytkownik systemu łączący się z sieci rozległej z systemem informatycznym ADO znajdującym się w sieci lokalnej, lub pracujący zdalnie na danych poza siedzibą ADO,
19) **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. dyskietka, dysk twardy, pendrive.

Użyte w niniejszej polityce pojęcia należy odnosić również do obowiązującej Instrukcji Zarządzania Systemem Informatycznym, a także do wydanych upoważnień do przetwarzania danych osobowych. Natomiast pojęcia opisane w przywołanej Instrukcji należy odnosić odpowiednio do Polityki Bezpieczeństwa.

4 WYKAZ BUDYNKÓW I POMIESZCZEŃ TWORZĄCYCH OBSZAR BEZPIECZNY

Miejsca przetwarzania poszczególnych zbiorów danych osobowych opisane są w Wykazie zbiorów danych osobowych stanowiącym załącznik nr 4 do niniejszej Polityki.

5 WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Wykaz przetwarzanych zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych znajduje się w Rejestrze czynności przetwarzania stanowiącym załącznik nr 1 do niniejszej Polityki oraz załącznik nr 4.

6 OPIS STRUKTURY ZBIORÓW DANYCH

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych znajduje się w Rejestrze czynności przetwarzania stanowiącym załącznik nr 1 do niniejszej Polityki.

7 ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZY PRZETWARZANIU DANYCH

Dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych ADO stosuje środki techniczne i organizacyjne właściwe dla wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, stosownie do wymogów określonych w Rozporządzeniu i RODO. Ocenę skutków dla ochrony danych osobowych

(DPIA) przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych .DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych lub administrator danych samodzielnie lub przy pomocy IOD.

7.1 ZABEZPIECZENIA FIZYCZNE OBSZARU BEZPIECZNEGO

- Pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz, w przypadku opuszczenia pomieszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych.
- Ekrany monitorów stanowisk dostępu do danych osobowych muszą zostać wyłączone po 5 minutach nieaktywności pracownika. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych będą ustawione w sposób uniemożliwiający tym osobom wgląd do danych.
- Dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pliki tekstowe, zewnętrzne nośniki danych) po zakończeniu pracy są przechowywane w zamykanych szafach – polityka czystego biurka.
- Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych : pracownicy, rekrutacja, kontrahenci, dane przekazane przez kontrahentów posiada system alarmowy – ogólny dla całego budynku .Obiekt objęty jest też całodobową ochroną fizyczną.
- Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętych niemetalowych szafach.
- Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą wolnostojących gaśnic znajdujących się w korytarzach budynku.
- Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów lub w inny ustalony sposób.

7.2 ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

- Zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
- Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
- Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
- Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
- Użyto system Firewall do ochrony dostępu do sieci komputerowej.

7.3 ZABEZPIECZENIA ORGANIZACYJNE

- Został powołany Inspektor Ochrony Danych
- Została opracowana i wdrożona polityka bezpieczeństwa oraz Instrukcja Zarządzania Systemem Informatycznym,
- Wszystkie osoby posiadające dostęp do danych osobowych posiadają pisemne upoważnienie ADO według wzoru stanowiącego załącznik nr 2 do niniejszej Polityki oraz prowadzona jest ewidencja osób upoważnionych do przetwarzania danych zawierająca:
  - imię i nazwisko osoby upoważnionej,
  - datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
  - stanowisko
  - nazwa zbiorów

  Ewidencja prowadzona jest wg wzoru stanowiącego załącznik nr 3 do niniejszej Polityki.

- Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
- Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
- Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy i podpisały stosowne oświadczenie według wzoru stanowiącego załącznik nr 2 do niniejszej Polityki .

8 UDOSTĘPNIANIE DANYCH I WSPÓŁPRACA Z PODMIOTAMI TRZECIMI

8.1 UDOSTĘPNIANIE DANYCH

Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa. Zbiory danych udostępnia się zgodnie z załącznikiem nr 13 na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.

Wniosek jest rozpatrywany przez Administratora Danych, który jednocześnie prowadzi ewidencję wniosków. Decyzję w sprawie udostępnienia danych podejmuje wyłącznie Administrator Danych.

Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli:

1. Spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób.
2. Dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania Wnioskodawcy.

8.2 POWIERZENIE PRZETWARZANIA

Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej. Podmiot, któremu ADO powierzył dane, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych, oraz jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie, w jakim reguluje to zawarta umowa.

Odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na Administratorze Danych Osobowych, co nie wyłącza w żadnym przypadku odpowiedzialności podmiotu, z którym zawarto umowę, z tytułu przetwarzania danych niezgodnie z ustawą.

Lista podmiotów, którym ADO powierzył do przetwarzania dane osobowe znajduje się w załączniku nr 4 do niniejszej polityki.

9 INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1) Każdy pracownik Administratora w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub Administratora danych.
2) Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

(a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
(b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
(c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)

3) Do typowych incydentów bezpieczeństwa danych osobowych należą:

(a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
(b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
(c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)

4) W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych prowadzi postępowanie wyjaśniające w toku, którego:
a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki
b) inicjuje ewentualne działania dyscyplinarne
c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości
d) dokumentuje prowadzone postępowania

5) W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych prowadzi postępowanie wyjaśniające w toku, którego:
a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały
b) zabezpiecza ewentualne dowody
c) ustala osoby odpowiedzialne za naruszenie
d) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody)
e) inicjuje działania dyscyplinarne
f) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości
g) dokumentuje prowadzone postępowania

10 ODPOWIEDZIALNOŚĆ PRACOWNIKÓW I ADMINISTRATORA

Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
Pracownicy ponoszą pełną odpowiedzialność za ochronę powierzonych im danych osobowych.
Z tytułu umowy o pracę lub innych umów cywilno-prawnych pracownik obciążony jest odpowiedzialnością za wywiązywanie się z własnych obowiązków oraz za potencjalne szkody wyrządzone pracodawcy.
Pracownik przyjmuje do wiadomości następujące kary wynikające z przepisów prawa:
Art. 266 Kodeksu karnego – Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
Art. 267 Kodeksu karnego – Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Tej samej karze podlega, kto informację uzyskaną w sposób określony powyżej ujawnia innej osobie.
Art. 268 Kodeksu karnego – Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli czyn dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. Kto, dopuszczając się czynu, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269a Kodeksu karnego – Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b Kodeksu karnego – Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.

Art. 82 ustęp 1 RODO – Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

Art. 82 ustęp 2 RODO – Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

Art. 82 ustęp 4 RODO – Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

Art. 82 ustęp 5 RODO – Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2.

Inne osoby mające dostęp do danych firmowych w tym danych osobowych ponoszą odpowiedzialność na podstawie odrębnych umów gwarantujących im dostęp, lub na podstawie przepisów ogólnych.

11 Załączniki

Załącznik nr 1 – Rejestr czynności przetwarzania
Załącznik nr 2 – Upoważnienie do przetwarzania danych osobowych
Załącznik nr 3 – Ewidencja osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 4 – Rejestr zbiorów danych
Załącznik nr 5 – Raport z naruszenia ochrony danych
Załącznik nr 6 – Rejestr naruszeń bezpieczeństwa
Załącznik nr 7 – Zgłoszenie naruszenia do UODO
Załącznik nr 8 – Komunikat o naruszeniu
Załącznik nr 9 – Karta szkolenia
Załącznik nr 10 – Wzór umowy powierzenia
Załącznik nr 11- Wzór klauzul informacyjnej
Załącznik nr 12 – Rejestr podmiotów przetwarzających
Załącznik nr 13 – Procedury związane z prawami jednostki w zakresie ochrony danych osobowych
Załącznik nr 14 – Procedura związana z zabezpieczeniem komputerów
Załącznik nr 15 – Procedura związana z usunięciem nośników
Załącznik nr 16 - Polityka Zarządzania Ryzykiem w procesach przetwarzania danych osobowych w Urzędzie Miasta i Gminy Mikołajki

Załącznik nr 1

REJESTR CZYNNOŚCI PRZETWARZANIA w Urzędzie Miasta i Gminy w Mikołajkach		
Lp.	**Opis pola informacyjnego**	**Dane**
1.	**Nazwa administratora danych:**	Urząd Miasta i Gminy w Mikołajkach
2.	**Dane kontaktowe administratora:**	ul. Kolejowa 7, 11-730 Mikołajki
	Proces 1	
1.	**Cel przetwarzania danych:**	Obsługa kadrowo-księgowa
2.	**Zbiór danych:**	Pracownicy, Rejestr VAT, rejestr osób wpłacających, ewidencja dzierżawców
3.	**Kategorie danych przetwarzane w procesie:**	imiona, nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania i pobytu, zameldowania, numer pesel, numer nip , miejsca pracy, zawodu, wykształcenia, seria i numer dowodu, numer telefonu, e-mail, poprzedni okres zatrudnienia, informacja dotycząca stopnia niepełnosprawności , przynależność do urzędu skarbowego, data ważności szkoleń i badań kontrolnych/okresowych , informacje o dodatkowych uprawnieniach, stan rodziny, orzeczenia w postepowaniu sądowym lub egzekucyjnym
4.	**Kategorie odbiorców danych:**	podmioty udzielające świadczenia zdrowotne, podmiot organizujący szkolenia w zakresie BHP, firmy szkoleniowe, zakłady ubezpieczeń i brokerzy ubezpieczeniowi, podmioty wydające karty sportowe, podmioty wydającym służbowe karty kredytowe, instytucje finansowe, Ministerstwo Finansów-na mocy ustawy Sąd- postępowanie egzekucyjne oraz inne podmioty upoważnione na podstawie przepisów prawa,

5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie będą przekazywane do państw trzecich
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 2	
1.	**Cel przetwarzania danych:**	Wykonywanie zadań z zakresu ewidencji ludności
2.	**Zbiór danych:**	Ewidencja ludności
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Nr PESEL, Nr NIP, informacje o skazaniu, inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym – orzeczenie o ubezwłasnowolnieniu, decyzje administracyjne
4.	**Kategorie odbiorców danych:**	Podmioty publiczne na podstawie przepisów
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 3	
1.	**Cel przetwarzania danych:**	Dane będą przetwarzane w celu: • wydania dowodu osobistego. • unieważnienia dowodu osobistego z powodu: – zgłoszenia utraty lub uszkodzenia dowodu, – zmiany danych zawartych w dowodzie, – upływu terminu ważności dowodu,

		– utraty obywatelstwa polskiego lub zgonu. • uzyskania zaświadczenia o danych własnych zgromadzonych w Rejestrze Dowodów Osobistych Dane będą przetwarzane na podstawie przepisów ustawy o dowodach osobistych.
2.	**Zbiór danych:**	Rejestr Dowodów Osobistych
3.	**Kategorie danych przetwarzane w procesie:**	Dane będą przetwarzane na podstawie przepisów ustawy o dowodach osobistych imiona i nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Nr PESEL, seria i nr dowodu osobistego
4.	**Kategorie odbiorców danych:**	W celu sporządzenia dowodu osobistego dane osobowe będą przekazywane do Centrum Personalizacji Dokumentów MSWiA. Ponadto dane mogą być udostępniane zgodnie z przepisami ustawy o dowodach osobistych służbom, organom administracji publicznej, prokuraturze oraz innym podmiotom, jeżeli wykażą w tym interes prawny w otrzymaniu danych.
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego Dane dotyczące utraconego dowodu osobistego (skradzionego lub zagubionego) będą przekazywane do Systemu Informacyjnego Schengen II na podstawie ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym. Dane będą przekazywane za pośrednictwem Krajowego Systemu Informatycznego prowadzonego przez Komendanta Głównego Policji.
6.	**Planowany termin usunięcia danych:**	Dane w Rejestrze Dowodów Osobistych przechowywane są bezterminowo

7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 4	
1.	**Cel przetwarzania danych:**	Realizacja obowiązku lustracji
2.	**Zbiór danych:**	Oświadczenia o stanie majątkowym
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, miejsce pracy, inne: informacja o stanie majątkowym, posiadaniu udziałów w spółkach, fundacjach, spółdzielniach, informacja o członkostwie w radzie nadzorczej, zarządzie, informacje odnośnie posiadanych nieruchomości, zadłużenie, mienie ruchome powyżej 10 000zł, kredyty
4.	**Kategorie odbiorców danych:**	urząd skarbowy, wojewoda – na podstawie ustawy „informacje jawne, ogólnodostępne (oprócz adresu i miejsca położenia nieruchomości) – na podstawie ustawy"
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie będą przekazywane do państw trzecich
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 5	
1.	**Cel przetwarzania danych:**	Dane mogą być przetwarzane w celu: sporządzenia aktu urodzenia dziecka sporządzenia aktu małżeństwa sporządzenia aktu zgonu przyjęcia oświadczeń o uznaniu ojcostwa i realizacji wniosku o wydanie zaświadczenia

		potwierdzającego uznanie ojcostwa przyjęcia oświadczenia rozwiedzionego małżonka o powrocie do nazwiska noszonego przed zawarciem małżeństwa przyjęcia oświadczeń o nazwisku pierwszego dziecka małżonków przy sporządzaniu aktu urodzenia przyjęcia oświadczeń małżonków, że dziecko jednego z małżonków będzie nosiło takie samo nazwisko, jakie nosi albo nosiłoby ich wspólne dziecko przyjęcia oświadczeń o zmianie imienia lub imion wydania zaświadczenia o stanie cywilnym wydania odpisu aktu stanu cywilnego wydania zaświadczenia do zawarcia małżeństwa za granicą wydania zaświadczenia o zaginięciu lub zniszczeniu ksiąg stanu cywilnego/wydania zaświadczenia o nieposiadaniu księgi stanu cywilnego sprostowania, uzupełnienia, unieważnienia aktu stanu cywilnego realizacji wniosku o sporządzenie polskiego aktu stanu cywilnego na podstawie zagranicznego dokumentu stanu cywilnego lub innych dokumentów potwierdzających urodzenie/małżeństwo/zgon za granicą realizacji wniosku o zezwolenie na zawarcie małżeństwa przed upływem terminu, o którym mowa w art. 4 ustawy Kodeks rodzinny i opiekuńczy realizacji wniosku o wydanie zaświadczenia o przyjętych sakramentach realizacji wniosku o zmianę imienia lub nazwiska. dołączenia do aktu stanu cywilnego wzmianki dodatkowej lub zamieszczenia przypisku przy akcie wydania dokumentów z akt zbiorowych

		zameldowania nadania numeru PESEL. Dane osobowe z rejestru stanu cywilnego stanowią podstawę wpisów w rejestrze PESEL. Dane osobowe będą przetwarzane na podstawie przepisów ustawy Prawo o aktach stanu cywilnego oraz przepisów ustawy o zmianie imienia i nazwiska.
2.	**Zbiór danych:**	Baza Usług Stanu Cywilnego Dane do rejestru stanu cywilnego wprowadzane są przez następujące organy: - kierownik urzędu stanu cywilnego sporządzający akt urodzenia, małżeństwa i zgonu oraz wprowadzający do nich zmiany; - kierownik urzędu stanu cywilnego wydający decyzję o zmianie imienia lub nazwiska
3.	**Kategorie danych przetwarzane w procesie:**	Dane osobowe będą przetwarzane na podstawie przepisów ustawy Prawo o aktach stanu cywilnego oraz przepisów ustawy o zmianie imienia i nazwiska. imiona i nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Nr PESEL, inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym – wyroki rozwodowe, decyzje administracyjne
4.	**Kategorie odbiorców danych:**	Kierownik urzędu stanu cywilnego udostępnia dane z rejestru stanu cywilnego wydając uprawnionym podmiotom dokumenty określone w ustawie – Prawo o aktach stanu cywilnego. Dostęp do danych mają także służby. Dane osobowe z rejestru stanu cywilnego stanowią podstawę wpisów w rejestrze PESEL.
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane dotyczące urodzeń, małżeństw i zgonów mogą być przekazywane do państw trzecich na podstawie umów

		międzynarodowych, których stroną jest Rzeczpospolita Polska.
6.	**Planowany termin usunięcia danych:**	Akty stanu cywilnego oraz akta zbiorowe rejestracji stanu cywilnego kierownik urzędu stanu cywilnego przechowuje przez okres: 1) 100 lat – akty urodzenia oraz akta zbiorowe rejestracji stanu cywilnego dotyczące aktu urodzenia; 2) 80 lat – akty małżeństwa, akty zgonu oraz akta zbiorowe rejestracji stanu cywilnego dotyczące aktu małżeństwa i aktu zgonu.
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 6	
1.	**Cel przetwarzania danych:**	Rozliczenia należności podatkowych
2.	**Zbiór danych:**	Ewidencja podatników, płatników i dłużników
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, Nr PESEL, Nr NIP, seria i nr dowodu osobistego, nr tel., inne: adres e-mail, dane dot. gruntów i budynków, dane finansowe, akty notarialne, stan zdrowia, inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym – decyzje administracyjne
4.	**Kategorie odbiorców danych:**	Komornicy sądowi, urząd skarbowy, poborca skarbowy, Firma odbierająca odpady komunalne, ZUS, KRUS, uczelnie ,banki, Prokuratura , Policja (na wniosek)

5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 7	
1.	**Cel przetwarzania danych:**	Wykonanie obowiązku kwalifikacji wojskowej
2.	**Zbiór danych:**	Rejestracja i kwalifikacja wojskowa (rejestr przedpoborowych i poborowych)
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Nr PESEL, seria i nr dowodu osobistego, inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym – decyzje administracyjne
4.	**Kategorie odbiorców danych:**	Wojsko – na mocy ustawy
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 8	
1.	**Cel przetwarzania danych:**	Prowadzenie ewidencji osób prowadzących działalność gospodarczą
2.	**Zbiór danych:**	Ewidencja działalności gospodarczej
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub

		pobytu, Nr PESEL, Nr NIP, miejsce pracy
4.	**Kategorie odbiorców danych:**	Podmioty publiczne na podstawie przepisów Osoby fizyczne ZUS, KRUS, uczelnie ,banki, Prokuratura , Policja (na wniosek)
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 9	
1.	**Cel przetwarzania danych:**	Prowadzenie rejestru osób będących użytkownikami wieczystymi gruntów, dzierżawcami lub najemcami gruntów Gminy
2.	**Zbiór danych:**	Ewidencje użytkowników wieczystych gruntów, dzierżawców i najemców
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, adres zamieszkania lub miejsce pobytu, PESEL, NIP, seria i numer dowodu osobistego, nr telefonu, adres e-mail
4.	**Kategorie odbiorców danych:**	Podmioty publiczne na podstawie przepisów
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Bezterminowe
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 10	
1.	**Cel przetwarzania danych:**	Wydawanie i prowadzenie rejestru zezwoleń na wykonanie zarobkowego transportu drogowego

2.	**Zbiór danych:**	Licencje uprawniające do wykonania zarobkowego transportu drogowego
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Nr PESEL, Nr NIP, nr tel., adres e-mail, nazwisko rodowe matki, inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym – decyzje (licencja)
4.	**Kategorie odbiorców danych:**	Podmioty publiczne na podstawie przepisów
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 11	
1.	**Cel przetwarzania danych:**	Ewidencja osób uiszczających opłaty lokalne
2.	**Zbiór danych:**	Opłaty lokalne
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, adres zamieszkania lub pobytu, Nr NIP, numer telefonu i adres e-mail ,inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym – decyzje administracyjne
4.	**Kategorie odbiorców danych:**	Komornicy sądowi, urząd skarbowy, poborca skarbowy
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 12		
1.	**Cel przetwarzania danych:**	Wydanie oraz ewidencjonowanie decyzji o zajęciu pasa ruchu drogowego i wbudowaniu urządzeń, wydawanie i ewidencjonowanie decyzji zezwalających na lokalizację zjazdu oraz lokalizację urządzeń i sieci w pasie drogowym lub działkach gminnych
2.	**Zbiór danych:**	Decyzje o zajęciu pasa ruchu drogowego oraz wbudowaniu urządzeń, decyzje zezwalające na lokalizację zjazdu oraz lokalizację urządzeń i sieci w pasie drogowym lub działkach gminnych
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, adres zamieszkania lub pobytu, PESEL nr tel., adres e-mail, inne
4.	**Kategorie odbiorców danych:**	Podmioty publiczne na podstawie przepisów
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 13		
1.	**Cel przetwarzania danych:**	Prowadzenie rejestru osób prowadzących turystyczną działalność gospodarczą
2.	**Zbiór danych:**	Ewidencja obiektów turystycznych
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, adres zamieszkania lub pobytu, Nr NIP, nr tel., adres e-mail
4.	**Kategorie odbiorców danych:**	Podmioty publiczne na podstawie przepisów, Osoby fizyczne
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 14		
1.	**Cel przetwarzania danych:**	Wydawanie i ewidencjonowanie zezwoleń na sprzedaż alkoholu
2.	**Zbiór danych:**	Zezwolenia na sprzedaż alkoholu
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, adres zamieszkania lub pobytu, Nr NIP, nr tel., adres e-mail, inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym – decyzje administracyjne
4.	**Kategorie odbiorców danych:**	Podmioty publiczne na podstawie przepisów Osoby fizyczne
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 15		
1.	**Cel przetwarzania danych:**	Wydawanie oraz ewidencjonowanie decyzji/protokołów/zgłoszeń na wycinkę drzew, decyzji o środowiskowych uwarunkowaniach, prowadzenie rejestru przedsiębiorców prowadzących odbiór i zagospodarowanie odpadów komunalnych(rejestr działalności regulowanej), prowadzenie rejestru przedsiębiorców opróżniających zbiorniki bezodpływowe i prowadzących transport nieczystości ciekłych .
2.	**Zbiór danych:**	Ochrona środowiska
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, adres zamieszkania lub pobytu, nr tel., adres e-mail, inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym – decyzje administracyjne
4.	**Kategorie odbiorców danych:**	Podmioty publiczne na podstawie przepisów Osoby fizyczne
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 16		
1.	**Cel przetwarzania danych:**	Przeprowadzenie i realizacja postępowania o udzielenie zamówienia publicznego
2.	**Zbiór danych:**	Zamówienia publiczne
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, data urodzenia, adres zamieszkania lub pobytu, Nr NIP, wykształcenie, seria i nr dowodu osobistego, nr tel., adres

		e-mail, uprawnienia, sytuacja finansowa, informacje o skazaniu
4.	**Kategorie odbiorców danych:**	Inspektor nadzoru inwestorskiego, autorskiego
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa
	Proces 17	
1.	**Cel przetwarzania danych:**	Wydawanie oraz ewidencjonowanie decyzji o warunkach zabudowy, decyzji o ustaleniu inwestycji celu publicznego, ewidencji budynków, wydawanie decyzji na podział nieruchomości
2.	**Zbiór danych:**	rejestr wydanych decyzji o warunkach zabudowy, rejestr wydanych decyzji celu publicznego, wykaz decyzji o podziale nieruchomości
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, adres zamieszkania lub pobytu, nr tel., adres e-mail, inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym – decyzje administracyjne
4.	**Kategorie odbiorców danych:**	Podmioty publiczne na podstawie przepisów Osoby fizyczne , Kancelaria prawna
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 18		
1.	**Cel przetwarzania danych:**	Wydawanie oraz ewidencjonowanie decyzji o dofinansowaniu dokształcania młodocianych pracowników, prowadzenie rejestru żłobków, prowadzenie rejestru jednostek oświatowych, dokonywanie wpisu do ewidencja niepublicznych placówek oświatowych, ewidencja oraz kontrola spełniania obowiązek nauki przez dzieci zamieszkałe na terenie Gminy Mikołajki, wydawanie oraz ewidencjonowanie decyzji o nadaniu awansu zawodowego nauczyciela, prowadzenie postępowania konkursowego na dyrektora szkoły, wydawanie zezwoleń na prowadzenie publicznych szkół, których organem prowadzącym jest inna osoba prawna lub osoba fizyczna, przygotowywanie umów dot. zwrotu kosztów dowozu dziecka niepełnosprawnego do placówki oświatowej, realizacja programów rządowych, obsługa kadrowa kierowników jednostek oświatowych,
2.	**Zbiór danych:**	Oświata (decyzje stypendialne, decyzje o dofinansowaniu dokształcania młodocianych pracowników, rejestr żłobków, rejestr jednostek oświatowych, rejestr uczniów podlegających obowiązkowi nauki, rejestr aktów nadania awansu zawodowego, rejestr niepublicznych placówek oświatowych, listy wypłat)
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, imiona i nazwiska rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Nr PESEL, Nr NIP, miejsce pracy, zawód, wykształcenie, seria i nr dowodu osobistego, nr tel., adres e-mail, sytuacja finansowa, informacje o stopniu niepełnosprawności inne orzeczenia wydane w postępowaniu sądowym, administracyjnym, egzekucyjnym –

		decyzje administracyjne, data ważności badań okresowych, stan rodzinny,
4.	**Kategorie odbiorców danych:**	instytucje państwowe, kancelarie prawne, podmioty udzielające świadczenia zdrowotne oraz inne podmioty upoważnione na podstawie przepisów prawa
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 19		
1.	**Cel przetwarzania danych:**	Zawieranie i wykonywanie umów
2.	**Zbiór danych:**	Zleceniobiorcy, Kontrahenci , j.s.t, jednostki administracji rządowej
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, adres zamieszkania lub pobytu, Nr NIP, seria i nr dowodu osobistego, nr tel., adres e-mail, PESEL
4.	**Kategorie odbiorców danych:**	Zgodnie z przepisami
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 20		
1.	**Cel przetwarzania danych:**	Przyjmowanie, rozpatrywanie i ewidencjonowanie skarg i wniosków

2.	**Zbiór danych:**	Skargi i wnioski
3.	**Kategorie danych przetwarzane w procesie:**	imiona i nazwiska, adres zamieszkania lub pobytu, nr tel., adres e-mail
4.	**Kategorie odbiorców danych:**	Kancelaria prawna, Radni Rady Miejskiej w Mikołajkach (członkowie Komisji Ds. Rozpatrywania Skarg i Wniosków, członkowie Komisji Rewizyjnej), Wojewoda
5.	**Państwo trzecie, do którego przekazuje się dane:**	Dane nie są przekazywane do państwa trzeciego
6.	**Planowany termin usunięcia danych:**	Zgodnie z przepisami
7.	**Opis zabezpieczeń technicznych:**	Wynika z Polityki Bezpieczeństwa
8.	**Opis zabezpieczeń organizacyjnych:**	Wynika z Polityki Bezpieczeństwa

Proces 21	
Cel przetwarzania danych:	Dodatkowe zadania podejmowane w ramach profilaktyki alkoholowej
Zbiór danych:	Zastosowanie obowiązku poddania się leczeniu odwykowemu
Kategorie danych przetwarzane w procesie:	imiona i nazwiska, adres zamieszkania lub pobytu, nr tel
Kategorie odbiorców danych:	Podmioty publiczne na podstawie przepisów Osoby fizyczne
Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
Planowany termin usunięcia danych:	Zgodnie z przepisami
Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 22

Cel przetwarzania danych:	Obsługa księgowa i bankowa
Zbiór danych:	Kontrahenci i pracownicy
Kategorie danych przetwarzane w procesie:	imiona i nazwiska, adres zamieszkania lub pobytu, Nr NIP, Regon, nr rachunku bankowego
Kategorie odbiorców danych:	Komornicy sądowi, urząd skarbowy, poborca skarbowy, banki
Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
Planowany termin usunięcia danych:	Zgodnie z przepisami
Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa
Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Proces 23	
Cel przetwarzania danych:	Wykonywanie zadań z zakresu ewidencji Radnych Rady Miejskiej w Mikołajkach i członków klubów radnych. Wykonywanie zadań z zakresu ewidencji sołtysów i członków rad sołeckich
Zbiór danych:	Ewidencja Radnych Rady Miejskiej w Mikołajkach i członków klubu radnych Ewidencja sołtysów i członków rad sołeckich
Kategorie danych przetwarzane w procesie:	imiona i nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Nr PESEL, nr tel., adres e-mail, wykształcenie, miejsce pracy, zawód
Kategorie odbiorców danych:	Biuro Rady Miejskiej w Mikołajkach/sekretariat
Państwo trzecie, do którego przekazuje się dane:	Dane nie są przekazywane do państwa trzeciego
Planowany termin usunięcia danych:	Zgodnie z przepisami
Opis zabezpieczeń technicznych:	Wynika z Polityki Bezpieczeństwa

Opis zabezpieczeń organizacyjnych:	Wynika z Polityki Bezpieczeństwa

Załącznik nr 2

Numer upoważnienia: ...../2018

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Danych występujący pod nazwą **URZĄD MIASTA I GMINY W MIKOŁAJKACH** ul. Kolejowa 7 11-730 Mikołajki (dalej Administrator Danych), na mocy delegacji uprawnienia do nadawania upoważnień wynikających z uprawnień Administratora Danych, na podstawie art. 29 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) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR),** niniejszym upoważniam do przetwarzania danych osobowych w formie papierowej oraz systemach informatycznych :

Imię i nazwisko osoby upoważnianej	Zbiory danych objęte zakresem upoważnienia	Data nadania upoważnienia
		.2018 rok

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

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami RODO i obowiązującymi u Administratora Danych wewnętrznymi regulacjami 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 lub odpowiedzialności cywilnej.

Oświadczenie

Oświadczam, że zapoznałam/em się – w zakresie wynikającym z przydzielonych zadań – z obowiązującymi w odniesieniu do ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi u Administratora Danych .Przyjmuję do wiadomości zawarte w nich obowiązki dotyczące ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po ustaniu zatrudnienia lub współpracy.

Data i podpis upoważniającego	Data i podpis osoby upoważnionej

Załącznik nr 3

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Stanowisko	Nazwy zbiorów objętych zakresem upoważnienia
1					
2					
3					
4					
5					
6					
7					
8					
9					

Załącznik nr 4

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Lp.	Nazwa zbioru - opis	Cel przetwarzania	Program	Wykaz pomieszczeń/budynków
1.	**Pracownicy**	Obsługa kadrowo-księgowa	1.Pakiet dla administracj i U.I. Infosystem: Księgowość budżetowa, Środki trwałe 2. IBank Corporate Banking 3.OPTIVUM -płace 4.ZETO PUMA - płace 5. PŁATNIK	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Księgowość – pokój 105 Kadry i płace – pokój 101
2.	**Baza Usług Stanu Cywilnego**	sporządzenia aktu urodzenia dziecka sporządzenia aktu małżeństwa sporządzenia aktu zgonu przyjęcia oświadczeń o uznaniu ojcostwa i realizacji wniosku o wydanie zaświadczenia potwierdzającego uznanie ojcostwa przyjęcia oświadczenia rozwiedzionego małżonka o powrocie do nazwiska noszonego przed zawarciem małżeństwa przyjęcia oświadczeń o nazwisku pierwszego dziecka małżonków przy sporządzaniu aktu urodzenia przyjęcia oświadczeń małżonków, że dziecko jednego z małżonków będzie nosiło takie samo nazwisko, jakie nosi albo nosiłoby ich wspólne dziecko przyjęcia oświadczeń o zmianie imienia lub imion wydania zaświadczenia o stanie cywilnym wydania odpisu aktu stanu cywilnego wydania zaświadczenia do zawarcia małżeństwa za granicą	Baza Usług Stanu Cywilnego w aplikacji ZRÓDŁO	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 1

		wydania zaświadczenia o zaginięciu lub zniszczeniu ksiąg stanu cywilnego/wydania zaświadczenia o nieposiadaniu księgi stanu cywilnego sprostowania, uzupełnienia, unieważnienia aktu stanu cywilnego realizacji wniosku o sporządzenie polskiego aktu stanu cywilnego na podstawie zagranicznego dokumentu stanu cywilnego lub innych dokumentów potwierdzających urodzenie/małżeństwo/zgon za granicą realizacji wniosku o zezwolenie na zawarcie małżeństwa przed upływem terminu, o którym mowa w art. 4 ustawy Kodeks rodzinny i opiekuńczy realizacji wniosku o wydanie zaświadczenia o przyjętych sakramentach realizacji wniosku o zmianę imienia lub nazwiska. dołączenia do aktu stanu cywilnego wzmianki dodatkowej lub zamieszczenia przypisku przy akcie wydania dokumentów z akt zbiorowych zameldowania . nadania numeru PESEL.		
3.	**Rejestr Dowodów Osobistych**	wydania dowodu osobistego. unieważnienia dowodu osobistego z powodu: zgłoszenia utraty lub uszkodzenia dowodu, zmiany danych zawartych w dowodzie, upływu terminu ważności dowodu, utraty obywatelstwa polskiego lub zgonu. uzyskania zaświadczenia o danych własnych zgromadzonych w Rejestrze Dowodów Osobistych Wydawanie dowodów osobistych	Rejestr Dowodów Osobistych w aplikacji ŹRÓDŁO	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 1
4.	**Oświadczenia o stanie majątkowym**	Realizacja obowiązku lustracji	Adobe Reader – publikacja	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 102 i 108

			Obsługa w wersji papierowej	
5.	**Ewidencja ludności i rejestr wyborców**	Prowadzenie spisu ludności Gminy	1.Źródło 2.ZETO PUMA – ewidencja ludności	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 5
6.	**Ewidencja podatników, płatników i dłużników**	Rozliczenia należności podatkowych	1.Pakiet dla administracj i U.I. Infosystem: Księgowość podatkowa, Księgowość zobowiązań, Egzekucje Auta 2. Info System GOMIG Odpady – Arisco 3.EWopis	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 4, 107
7.	**Rejestracja i kwalifikacja wojskowa (rejestr przedpoborowych i poborowych)**	Wykonanie obowiązku kwalifikacji wojskowej	Obsługa w wersji papierowej	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 113
8.	**Ewidencja działalności gospodarczej**	Prowadzenie ewidencji osób prowadzących działalność gospodarczą	1.CEIDG 2.ZETO PUMA	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 5
9.	**Ewidencja użytkowników wieczystych gruntów, dzierżawców i najemców**	Prowadzenie rejestru osób będących użytkownikami wieczystymi gruntów, dzierżawcami lub najemcami gruntów Gminy	1.EW Mapa 2.Program EW Opis 3. Pakiet dla administracj i U.I. Infosystem: dzierżawy	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 110
10.	**Rejestr korespondencji i rejestr faktur**	Ewidencja korespondencji ePUAP	1.Obsługa w wersji papierowej 2.ePUAP	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 102
11	**Licencje uprawniające do wykonania zarobkowego transportu drogowego**	Wydawanie i prowadzenie rejestru ewidencji do wykonania zarobkowego transportu drogowego	Obsługa w wersji papierowej	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 pokój 5

12	**Opłaty lokalne**	Ewidencja osób uiszczających opłaty lokalne	Pakiet dla administracj i U.I. Infosystem: Księgowość podatkowa	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 4
13	**Decyzje o zajęciu pasa ruchu drogowego oraz wbudowaniu urządzeń, decyzje zezwalające na lokalizację zjazdu oraz lokalizację urządzeń i sieci w pasie drogowym lub działkach gminnych**	Wydawanie oraz ewidencjonowanie decyzji o zajęciu pasa ruchu drogowego oraz wbudowaniu urządzeń, decyzji zezwalających na lokalizację zjazdu oraz lokalizację urządzeń i sieci w pasie drogowym lub działkach gminnych Wydanie oraz ewidencjonowanie decyzji o zajęciu pasa ruchu drogowego i wbudowaniu urządzeń	Program EW Mapa Program EW Opis	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 110, 113
14	**Ewidencja obiektów turystycznych**	Prowadzenie rejestru osób prowadzących turystyczną działalność gospodarczą	MS WORD + wersja papierowa	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 112
15	**Zezwolenia na sprzedaż alkoholu**	Wydawanie i ewidencjonowanie zezwoleń na sprzedaż alkoholu	ZETO PUMA	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 5
16	**Ochrona środowiska**	Wydawanie oraz ewidencjonowanie decyzji/ zgłoszeń/protokołów na wcinkę drzew, decyzji środowiskowych uwarunkowaniach, prowadzenie rejestru przedsiębiorców prowadzących odbiór i zagospodarowanie odpadów komunalnych, prowadzenie rejestru przedsiębiorców opróżniających zbiorniki bezodpływowe i transport nieczystości ciekłych.	ARISCO *baza ooś (program Ministerstwa Środowiska*	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 4
17	**Zamówienia publiczne**	Przeprowadzenie i realizacja postępowania o udzielenie zamówienia publicznego	Portal zamówień publicznych	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 114
18	**Zbiór decyzji o warunkach zabudowy, decyzji o ustaleniu inwestycji celu publicznego, ewidencji budynków, decyzji na podział nieruchomości**	Wydawanie oraz ewidencjonowanie decyzji o warunkach zabudowy, decyzji o ustaleniu inwestycji celu publicznego, ewidencji budynków, wydawanie decyzji na podział nieruchomości	Program EW Mapa Program EW Opis	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 110
19	**Oświata (decyzje stypendialne, decyzje o dofinansowaniu dokształcania**	Wydawanie oraz ewidencjonowanie decyzji o dofinansowaniu dokształcania młodocianych pracowników, prowadzenie rejestru	SIO	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7

	młodocianych pracowników, rejestr żłobków, rejestr jednostek oświatowych)	żłobków, prowadzenie rejestru jednostek oświatowych, dokonywanie wpisu do ewidencja niepublicznych placówek oświatowych, ewidencja oraz kontrola spełniania obowiązek nauki przez dzieci zamieszkałe na terenie Gminy Mikołajki, wydawanie oraz ewidencjonowanie decyzji o nadaniu awansu zawodowego nauczyciela, prowadzenie postępowania konkursowego na dyrektora szkoły, wydawanie zezwoleń na prowadzenie publicznych szkół, których organem prowadzącym jest inna osoba prawna lub osoba fizyczna, przygotowywanie umów dot. zwrotu kosztów dowozu dziecka niepełnosprawnego do placówki oświatowej, realizacja programów rządowych, obsługa kadrowa kierowników jednostek oświatowych,		Pokój 101
20	**Kontrahenci**	Zawieranie i wykonywanie umów Obsługa księgowa i bankowa	1.Pakiet dla administracj i U.I. Infosystem: Księgowość budżetowa Rejestr VAT 2.IBank Corporate Banking	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 105, kasa
	Kontrahenci, Zleceniobiorcy, Wykonawcy	Zawieranie i wykonywanie umów	1.ZETO PUMa - płace 2.PŁATNIK	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 101
21	**Skargi i wnioski**	Przyjmowanie, rozpatrywanie i ewidencjonowanie skarg i wniosków	word Ewidencja papierowa	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 102
22	**Ewidencja Radnych Rady Miejskiej w Mikołajkach i członków klubu radnych Ewidencja sołtysów i członków rad sołeckich**	Wykonywanie zadań z zakresu ewidencji Radnych Rady Miejskiej w Mikołajkach i członków klubów radnych. Wykonywanie zadań z zakresu ewidencji sołtysów i członków rad sołeckich	Ewidencja papierowa	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 108
23	**Rejestr VAT, rejestr osób wpłacających podatki, opłaty lokalne i pozostałe**	Wystawianie faktur, przyjmowanie wpłat, wypłaty, rozliczenia należności z tytułu dzierżaw i najmu	Pakiet dla administracj	Urząd Miasta i Gminy w

	opłaty, ewidencja dzierżawców		i U.I. Infosystem: Rejestr VAT Kasa Dzierżawy	Mikołajkach , ul. Kolejowa 7
24	**Informacje publiczne**	Przyjmowanie, rozpatrywanie i ewidencjonowanie skarg i wniosków	word Ewidencja papierowa	Urząd Miasta i Gminy w Mikołajkach , ul. Kolejowa 7 Pokój 102

Załącznik nr 5

Raport z naruszenia ochrony danych

1. Data ..... godzina .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub przepytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):

.....

3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

.....

4. Rodzaj naruszenia, zakres naruszenia:

.....

5. Określenie danych osobowych, jakich dotyczy zdarzenie i określenie okoliczności towarzyszących naruszeniu:

.....

..

6. Podjęte działania po wykryciu naruszenia:

.....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

.....

7. Postępowanie wyjaśniające i naprawcze:

.....

.....

.....

(podpis pracownika/osoby zgłaszającej) (podpis administratora)

Załącznik nr 6

REJESTR NARUSZEŃ BEZPIECZEŃSTWA

Naruszenie bezpieczeństwa – opis naruszenia	Źródło zgłoszenia – osoba/podmiot zgłaszający incydent	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za błąd/naruszenie lub informacja o braku takiej osoby	Przyczyna	Działanie zapobiegawcze / korygujące wraz ze wskazaniem osoby odpowiedzialnej za wykonanie	Ocena skuteczności podjętych działań

Dla .....

(dane administratora)

Załącznik nr 7

Urząd Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

ZGŁOSZENIE

W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 33 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu ... w ... .

1.	**Charakter naruszenia ochrony danych:**	Np. *Przesłanie przez pracownika wiadomości e-mail do błędnego adresata (nieznana osoba) zamiast do współpracownika wraz z załącznikiem w formacie pliku Excel (takie jak: imię i nazwisko, adres zamieszkania, PESEL, nr. dowodu tożsamości,, numer telefonu, adresy e-mail)*
2.	**Kategoria i przybliżona liczba osób, których dane dotyczą:**	Np.. *Liczba osób, których dane dotyczą .....*
3.	**Liczba wpisów, których dotyczy naruszenie:**	Np. *821*
4.	**Możliwe konsekwencje naruszenia ochrony danych:**	Np. *Powstanie szkód majątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub kradzież lub sfałszowanie tożsamości, strata finansowa*
5.	**Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:**	Np. *Wdrożenie stosownych środków kryptograficznych, w tym w tym pseudonimizacja, zakaz przesyłania załączników zawierających dane osobowe w sposób niezabezpieczony.*
6.	**Dane inspektora ochrony danych**	Np. *....., nr. telefonu: XXX XXX XXX, adres e-mail: iod@domena.pl*

.....

(podpis)

*W przypadku zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin, administrator danych zobowiązany jest do złożenia wyjaśnień w przedmiocie przyczyn opóźnienia.

....., dnia ..... r.

.....

(pieczęć Administratora)

Załącznik nr 8

Komunikat o naruszeniu ochrony danych

Komunikat o naruszeniu ochrony danych z dnia .....

1.	Charakter naruszenia ochrony danych:	
2.	Kategoria i przybliżona liczba osób, których dane dotyczą:	
3.	Liczba wpisów, których dotyczy naruszenie:	
4.	Możliwe konsekwencje naruszenia ochrony danych:	
5.	Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:	

.....

Załącznik nr 9

KARTA SZKOLENIA WSTĘPNEGO Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Imię i nazwisko osoby odbywającej szkolenie: .....
Stanowisko: .....
Instruktaż przeprowadzony: ..... (imię i nazwisko przeprowadzającego instruktaż)
W ramach szkoleniach poruszone zostały następujące tematy i zagadnienia:
Zgodnie z Polityką bezpieczeństwa informacji i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wymaga się tego, aby: 1) Dostęp do danych osobowych miały osoby posiadające upoważnienie do przetwarzania danych. 2) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu danych. 3) Dane były chronione przed dostępem do nich osób nieupoważnionych. 4) Pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz. 5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy. 6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W sytuacji, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia administratora danych. 7) Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy. 8) W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności. 9) Szafy, w których przechowywane są dane, powinny być zamykane na klucz. 10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy. 11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane. 12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do wykonania czynności służbowych, a następnie muszą być chowane do szaf. 13) Dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy. 14) Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane. 15) W razie potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane. 16) Nie należy udostępniać osobom nieupoważnionym tych komputerów. 17) W razie potrzeby przeniesienia danych osobowych pomiędzy komputerami należy zrobić to z zachowaniem szczególnej ostrożności. 18) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe. 19) Jeśli nie ma możliwości skasowania danych z nośnika (np. płyta CD-ROM), należy go zniszczyć fizycznie. 20) W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków. 21) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną. 22) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz. 23) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

Za prawidłowy nadzór przetwarzania danych oraz zapewnienie im odpowiedniej ochrony odpowiada każdy pracownik na swoim stanowisku pracy, zgodnie z obowiązkami pracowniczymi.
Za nieprzestrzeganie procedur bezpieczeństwa i naruszenie ochrony danych grozi odpowiedzialność finansowa, odszkodowawcza, dyscyplinarna, a w skrajnych przypadkach nawet karna.
Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia danych osobowych to głównie: 1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp., 2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy, 3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru, 4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów, lub inny komunikat o podobnym znaczeniu, 5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie, 6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych, 7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji), 8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie, 9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń, 10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp., 11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki itp., 12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane, 13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.).Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.
Uwagi: .....

Przeczytałem poniższy instruktaż, w pełni go zrozumiałem i zaakceptowałem. Zobowiązuję się go przestrzegać, co potwierdzam własnoręcznym podpisem*

.....

(data i podpis osoby, której udzielono instruktażu)

....

(administrator danych, nazwa, pieczątka) (miejscowość, data)

** Podpis jest potwierdzeniem odbycia instruktażu i zapoznania się z przepisami oraz zasadami przetwarzania i ochrony danych osobowych. Podpisaną kartę przechowuje dział kadr*

Załącznik nr 10

Umowa powierzenia przetwarzania danych osobowych
zawarta dnia 25-05-2018 r. pomiędzy:
(zwana dalej „Umową")

NIP: ....., REGON.....
reprezentowanym przez .....
zwany w dalszej części Umowy „Administratorem danych" lub „Administratorem"
oraz
.....
zwany w dalszej części Umowy „Podmiotem przetwarzającym"
reprezentowany przez:

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (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 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 dane zwykłe i szczególne w zakresie ..... Zakres przetwarzanych danych obejmuje w szczególności : imienia, nazwiska, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania i pobytu, numer pesel.
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy.

§ 3
Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

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 zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, o której mowa w art. 28 ust 3 pkt b Rozporządzenia przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający nie pobiera danych osobowych w związku z realizacją umowy n z zakresu serwisu informatycznego.
6. W miarę możliwości 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.

§ 4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy.
2. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 5

Podpowierzenie

1. Podmiot przetwarzający może powierzyć dane osobowe objęte Umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w § 5 ust. 1 Umowy, winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

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.

§ 7

Czas obowiązywania Umowy

Umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony.*

§ 8

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych 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.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

§ 10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.
2. W sprawach nieuregulowanych Umową zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.

Administrator danych: **Podmiot przetwarzający:**

Załącznik nr 11

Wzory Klauzul Informacyjnych RODO

Naszym celem jest zapewnienie bezpieczeństwa przetwarzanych Państwa danych osobowych w strukturze Urzędu Miasta i Gminy w Mikołajkach zgodnie z Rozporządzeniem 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 (RODO), ustawą o ochronie danych osobowych z 2018 r. oraz aktami wykonawczymi.

Administratorem Danych Osobowych jest Burmistrz Miasta Mikołajki reprezentujący Urząd Miasta i Gminy Mikołajki, z siedzibą przy ul. Kolejowej 7, 11-730 Mikołajki.

Urząd Miasta i Gminy przetwarza dane osobowe na podstawie:
- art. 6 a) RODO - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
- art. 6 b) RODO - 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,
- art. 6 c) RODO przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Przetwarzając Państwa dane osobowe opieramy się na następujących zasadach:

Zasada przejrzystości zgodnie z którą wszelkie komunikaty związane z przetwarzaniem danych osobowych będą prezentowane w łatwo dostępny, zrozumiały sposób, a także jasnym i prostym językiem.

Zasada zgodności z prawem, która wymaga aby przetwarzanie danych osobowych było wykonywane na podstawie obowiązujących przepisów prawa związanych z realizacją uzasadnionego interesu Administratora Danych Osobowych.

Zasada ograniczenia celu przetwarzania danych osobowych, która wymaga aby dane były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Zasada minimalizacji danych, która wymaga aby dane osobowe były adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane.

Zasada prawidłowości danych, zgodnie z którą dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane.

Zasada ograniczenia przechowywania danych, która wymaga, aby okres przetwarzania danych był ograniczony do czasu jaki jest niezbędny do tego, aby osiągnąć założony cel przetwarzania danych. W szczególności zapewnienia ograniczenia okresu przechowywania danych zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. z 2011 r., Nr 14, poz. 67 ze zm.).

Zasada integralności i nienaruszalności zgodnie z którą dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich.

KLAUZULA INFORMACYJNA OGÓLNA

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016, dalej jako Rozporządzenie) informuję, iż:

1) administratorem Pani/Pana danych osobowych jest **Burmistrz Miasta Mikołajki** reprezentujący Urząd Miasta i Gminy Mikołajki, z siedzibą przy ul. Kolejowej 7, 11-730 Mikołajki.

2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: iod24@gptogatus.pl

3. Państwa dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit a, b, c i art. 9 ust. 2 lit. g RODO oraz art. 7 ust. 1 ustawy o samorządzie gminnym jedynie w celu i zakresie niezbędnym do realizacji ustawowych zadań Gminy.

Art. 6 ust. 1 lit a,b,c RODO: 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;

art. 9 ust. 2 lit. g RODO: przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

4. Odbiorcami Państwa danych osobowych będą podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa oraz na podstawie umów powierzenia przetwarzania danych osobowych

5. Państwa dane osobowe będą przechowywane w czasie określonym przepisami prawa zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. 2011 nr 14 poz. 67 z późn. zm.).

6. Posiadają Państwa prawo żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, jak również prawo do wniesienia sprzeciwu wobec przetwarzania.

7. Jeżeli przetwarzanie odbywa się na podstawie wyrażonej przez Państwa zgody, to przysługuje Pani/Panu prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność przetwarzania z prawem.

Posiadają Państwa prawo wniesienia skargi do organu nadzorczego, Prezesa Urzędu Ochrony Danych.

Załącznik nr 12

Rejestr podmiotów przetwarzających

Lp.	Nazwa firmy	Zakres powierzonych danych	Cel powierzenia
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Załącznik nr 13

PROCEDURA 1

Prawo do ograniczenia przetwarzania danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 1	Realizacja prawa do ograniczenia przetwarzania danych osoby, której dane dotyczą	**Nr wersji procedury : 1.0**
		Ilość stron : 2

1. Uczestnicy procedury:

- wnioskodawca;
- osoba upoważniona do przetwarzania danych osobowych;
- Administrator Systemu Informatycznego;
- Administrator Danych.

2. Wymagane dokumenty:

- wniosek osoby, której dane dotyczą, o ograniczenie przetwarzania jego danych osobowych;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na wniosek.

3. Przesłanki warunkujące skuteczność żądania:

Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania w następujących przypadkach:

- osoba ta kwestionuje prawidłowość danych osobowych – na okres pozwalający sprawdzić prawidłowość tych danych;
- przetwarzanie jest niezgodne z prawem, a osoba ta sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- Administrator Danych nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne tej osobie do ustalenia, dochodzenia lub obrony roszczeń;
- osoba ta wniosła sprzeciw wobec przetwarzania jej danych – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora Danych są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

4. Procedura:

- rejestracja wniosku
- ustalenie zasadności żądania;
- przedstawienie propozycji działania Administratorowi danych;

- w przypadku żądania uzasadnionego (**pkt 3**):
    - powiadomić Administratora danych o konieczności ograniczenia przetwarzania danych,
    - na podstawie decyzji Administratora danych ograniczyć przetwarzanie tylko do przechowywania danych,
    - przygotować odpowiedź na żądanie i przedstawić ją do podpisu Administratorowi danych,
    - wysłać odpowiedź wnioskodawcy i poinformować o odbiorcach danych, jeżeli żądano tego we wniosku,
    - poinformować pisemnie odbiorców danych o decyzji ograniczenia przetwarzania,

W przypadku podjęcia decyzji o ograniczeniu przetwarzania danych – dane te można przetwarzać wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego;

5. W przypadku żądania nieuzasadnionego:

- sporządzić decyzję odmowną ograniczenia przetwarzania z uzasadnieniem,
- przedstawić decyzję do podpisu Administratorowi danych;
- przesłać decyzję wnioskodawcy listem poleconym.

PROCEDURA 2

Prawo dostępu do danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 2	Realizacja prawa dostępu do danych osobowych osoby, której dane dotyczą	**Nr wersji procedury : 1.0**
		Ilość stron : 1

1. Uczestnicy procedury:

- wnioskodawca
- osoby wyznaczone do realizacji prawa przez Administratora;
- Administrator Danych.

2. Wymagane dokumenty:

- wniosek o udostępnienie danych osobowych;
- wzór odpowiedzi na żądanie prawa dostępu do danych;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą.

3. Procedura:

- ujęcie wniosku na ewidencję;

- przygotowanie odpowiedzi na wniosek;
- przedstawienie Administratorowi danych wniosku do podpisu;
- wysłanie odpowiedzi do wnioskodawcy;
- dokonanie wpisu w ewidencji o wysłaniu odpowiedzi na wniosek.

4. Uwagi:

- udzielane informacje:
  - cele przetwarzania danych osobowych,
  - kategorie danych osobowych,
  - odbiorcy lub kategorie odbiorców danych,
  - planowany okres przechowywania danych osobowych lub kryteria ustalania tego okresu,
  - informacje o prawie do sprostowania danych, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
  - informacja o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w Warszawie,
  - informacja źródle pozyskania danych osobowych,
  - informacja o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu oraz istotne informacje o zasada ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

- wnioskodawcy dostarcza się kopie danych osobowych podlegających przetwarzaniu. Za kolejne kopie pobiera się opłatę, wynikającą z kosztów administracyjnych.

PROCEDURA 3

Prawo do sprostowania danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 3	Realizacja prawa do sprostowania danych osoby, której dane dotyczą	**Nr wersji procedury : 1.0**
		Ilość stron : 1

1. Uczestnicy procedury:

- wnioskodawca;
- osoba upoważniona do przetwarzania danych osobowych;
- Administrator Systemu Informatycznego;
- Administrator Danych.

2. Wymagane dokumenty:

- wniosek osoby, której dane dotyczą, o sprostowanie danych osobowych;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na wniosek;
- opcjonalnie – dodatkowe oświadczenie o przetwarzaniu danych osobowych.

3. Procedura:

- rejestracja wniosku ;
- sprostowanie nieprawidłowych danych osobowych w zbiorze przetwarzanym w systemie informatycznym lub przetwarzanym tradycyjnie;
- przygotowanie odpowiedzi na wniosek o sprostowaniu danych;
- przedstawienie odpowiedzi na wniosek do podpisu Administratorowi danych;
- przesłanie wnioskodawcy odpowiedzi na wniosek;
- opcjonalnie – przesłanie wnioskodawcy dodatkowego oświadczenia o przetwarzaniu danych osobowych;
- przesłać odbiorcom danych informację o decyzji sprostowania danych.

PROCEDURA 4

Prawo do usunięcia danych - bycia zapomnianym

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 4	Realizacja prawa do usunięcia danych - do bycia zapomnianym - osoby której dane dotyczą	**Nr wersji procedury : 1.0**
		Ilość stron : 2

1. Uczestnicy procedury:

- wnioskodawca;
- osoba upoważniona do przetwarzania danych osobowych;
- Administrator Systemu Informatycznego;
- Administrator Danych.

2. Wymagane dokumenty:

- wniosek osoby, której dane dotyczą, o usunięcie danych osobowych („bycia zapomnianym");
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na wniosek.

3. **Przesłanki warunkujące żądanie usunięcia danych („do bycia zapomnianym"):**

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie danych „zwykłych" lub „szczególnych kategorii" i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania jej danych osobowych:
    - w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych,
    - do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych, 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,
    - opartych na profilowaniu;

      i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,

    - na potrzeby marketingu bezpośredniego, w tym profilowania;

- dane osobowe są przetwarzane niezgodnie z prawem;
- dane osobowe muszą być usunięte w celu wywiązania się z obowiązku prawnego;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego oferowanych dziecku, które ukończyło 16 lat.

W przypadku upublicznienia danych osobowych Administratora Danych ma obowiązek usunąć te dane osobowe, podejmując w tym celu rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich repliki.

4. **Nieskuteczność żądania:**

Żądanie usunięcia danych („bycia zapomnianym") jest nieskuteczne w zakresie w jakim przetwarzanie jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych;
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego:
    - profilaktyki zdrowotnej, medycyny pracy, oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa lub zgodnie z umową z pracownikami służby zdrowia,
    - interes publiczny w dziedzinie zdrowia publicznego, taki jak ochrona przed zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa, które przewiduje odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową,

z zastrzeżeniem warunków i zabezpieczeń, że dane osobowe będą przetwarzane przez lub na odpowiedzialność pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa lub przepisów ustanowionych przez właściwe organy krajowe;

- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub dla celów statystycznych, o ile prawdopodobne jest, że realizacja prawa do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
- do ustalenia, dochodzenia lub obrony roszczeń.

5. Procedura:

- rejestracja wniosku;
- ustalenie zasadności żądania;
- w przypadku żądania uzasadnionego (**pkt 3**):
  - powiadomić Administratora danych o konieczności usunięcia danych,
  - na podstawie decyzji Administratora danych usunąć dane i powiadomić innych administratorów w przypadku upublicznienia danych,
  - przygotować odpowiedź na żądanie i przedstawić ją do podpisu Administratorowi danych,
  - wysłać odpowiedź wnioskodawcy i poinformować go o odbiorcach danych,
  - poinformować odbiorców danych o decyzji usunięcia danych;

- w przypadku żądania nieuzasadnionego (**pkt 4**):
  - powiadomić Kierownika Administratora danych o nieskuteczności żądania, z określeniem przyczyny,
  - przygotować odpowiedź na żądanie wnioskodawcy i przedstawić ją do podpisu Administratorowi danych,
  - wysłać odpowiedź wnioskodawcy.

PROCEDURA 5

Prawo do przenoszenia danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 5	Realizacja prawa do przenoszenia danych osoby, której dane dotyczą	**Nr wersji procedury : 1.0**
		Ilość stron : 2

1. Uczestnicy procedury:

- wnioskodawca
- osoba upoważniona do przetwarzania danych osobowych;

- Administrator Systemu Informatycznego;
- Administrator Danych.

2. Wymagane dokumenty:

- wniosek osoby, której dane dotyczą, o przeniesienie danych osobowych;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na wniosek.

3. Przesłanki warunkujące zasadność żądania:

Osoba, której dane dotyczą ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do druku dane osobowe jej dotyczące, które dostarczyła Administratorowi Danych, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane, jeżeli:

- przetwarzanie odbywa się na podstawie zgody lub umowy;
- przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora Danych bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

4. Nieskuteczność żądania:

- prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych;
- prawo do przenoszenia danych nie ma zastosowania w przypadku przetwarzania danych dla celów interesu publicznego w dziedzinie zdrowia publicznego takich, jak:
    - profilaktyka zdrowotna, medycyna pracy, ocena zdolności pracownika do pracy, diagnoza medyczna, zapewnienie opieki zdrowotnej lub zabezpieczenia społecznego, leczenie lub zarządzanie systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa lub zgodnie z umową z pracownikami służby zdrowia,
    - ochrona przed zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa, które przewiduje odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową,

Z zastrzeżeniem warunków i zabezpieczeń, że dane osobowe będą przetwarzane przez lub na odpowiedzialność pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa lub przepisów ustanowionych przez właściwe organy krajowe;

- prawo do przenoszenia danych nie ma zastosowania w przypadku przetwarzania danych dla celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub dla celów statystycznych, o ile prawdopodobne jest, że realizacja

prawa do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
- prawo do przenoszenia danych nie ma zastosowania w przypadku przetwarzania danych dla celów ustalenia, dochodzenia lub obrony roszczeń.

5. Procedura:

- rejestracja wniosku ;
- ustalenie zasadności żądania;
- przedstawienie propozycji działania Administratorowi danych;
- w przypadku żądania uzasadnionego (**pkt 3**):
  - powiadomić Administratora danych o konieczności przeniesienia danych,
  - na podstawie decyzji Administratora danych przygotować w ustrukturyzowanym, powszechnie używanym formacie nadającym się do druku dane osobowe dotyczące wnioskodawcy,
  - przesłać wnioskodawcy przygotowane dane lub bezpośrednio wskazanemu przez wnioskodawcę administratorowi,
  - poinformować pisemnie wnioskodawcę o sposobie realizacji wniosku;

- w przypadku żądania nieuzasadnionego (**pkt 4**):
  - sporządzić decyzję odmowną z uzasadnieniem,
  - przedstawić decyzję do podpisu Administratorowi danych;
  - przesłać decyzję wnioskodawcy listem poleconym za potwierdzeniem odbioru.

PROCEDURA 6

PRAWO DO SPRZECIWU NA ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI, W TYM PROFILOWANIE

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 6	Realizacja prawa do sprzeciwu na zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie	**Nr wersji procedury : 1.0**
		Ilość stron : 2

1. Uczestnicy procedury:

- wnioskodawca;
- osoba upoważniona do przetwarzania danych osobowych;
- Administrator Systemu Informatycznego;
- Administrator Danych.

2. **Wymagane dokumenty:**

- sprzeciw osoby, której dane dotyczą, na zautomatyzowane podejmowanie decyzji, w tym profilowanie;
- ewidencja udzielanych informacji w sprawach dotyczących praw osób, których dane dotyczą;
- odpowiedź na sprzeciw.

3. **Przesłanki warunkujące skuteczność sprzeciwu:**

- osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania jej danych celem:
  - wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
  - wynikającym z prawnie uzasadnionych interesów realizowanych przez administratora, 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, w tym profilowania. W takich przypadkach nie wolno już przetwarzać tych danych osobowych, chyba że wykaże się istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń;

- jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. W taki przypadku nie wolno już przetwarzać tych danych osobowych do takich celów;

- jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
- osoba, której dane dotyczą, ma prawo by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Uwagi:

- najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie do sprzeciwu w przypadku celów przetwarzania określonych w ust. 3 pkt 1 i 2
- osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

4. Nieskuteczność sprzeciwu:

W przypadku zautomatyzowanego przetwarzania danych osobowych, w tym profilowania sprzeciw jest nieskuteczny w przypadku:

- gdy decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
- gdy takie przetwarzanie danych jest dozwolone prawem i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą;
- jeżeli decyzja opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

Decyzje nie mogą opierać się na szczególnych kategoriach danych osobowych, chyba że osoba, której dane dotyczą wyraziła na to zgodę lub dane przetwarzane są ze względu na ważny interes publiczny.

5. Procedura:

- rejestracja sprzeciwu ;
- ustalenie zasadności sprzeciwu;
- przedstawienie propozycji decyzji Administratorowi danych;
- w przypadku sprzeciwu uzasadnionego (**pkt 3**):
  - powiadomić Administratora danych o konieczności zaprzestania przetwarzania danych,
  - zaprzestać przetwarzanie danych osobowych,
  - na podstawie decyzji Administratora danych przygotować odpowiedź na sprzeciw,
  - poinformować pisemnie osobę wnoszącą sprzeciw o sposobie realizacji żądania;

- w przypadku nieskuteczności sprzeciwu (**pkt 4**):
  - sporządzić decyzję odmowną z uzasadnieniem,
  - przedstawić decyzję do podpisu Administratorowi danych,
  - przesłać decyzję wnioskodawcy listem poleconym za potwierdzeniem odbioru

PROCEDURA 7

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 7	Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych	**Nr wersji procedury : 1.0**
		Ilość stron : 1

1. **Uczestnicy procedury:**

- Inspektor Ochrony Danych Osobowych;
- Administrator Danych.

2. **Wymagane dokumenty:**

- zawiadomienie o naruszeniu ochrony danych osobowych;
- ewidencja naruszeń ochrony danych osobowych.

3. **Wymagalność zawiadomienia osoby, której dane dotyczą:**

Zawiadomienie jest wymagane jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Zawiadomienie powinno jasnym i prostym językiem opisać charakter naruszenia ochrony danych osobowych oraz zawierać:

- imię i nazwisko Inspektora Ochrony Danych Osobowych oraz jego dane kontaktowe
- możliwe konsekwencje naruszenia ochrony danych osobowych
- środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych w tym środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

4. **Przypadki, w których nie jest wymagane zawiadomienie:**

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i zostały one zastosowane do danych osobowych, których dotyczy naruszenie – w szczególności takie jak szyfrowanie;
- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- zawiadomienie osoby, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku – w tym przypadku administrator wydaje publiczny komunikat lub stosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

5. **Procedura:**

- na podstawie raportu ASI opracować zawiadomienie osoby, której dane dotyczy, o naruszeniu ochrony jej danych;
- zarejestrować zawiadomienie w *Ewidencji naruszeń ochrony danych osobowych*;
- przedstawić zawiadomienie Administratorowi danych do podpisu;
- przesłać zawiadomienie listem poleconym za potwierdzeniem odbioru;
- drugi egzemplarz zarchiwizować w teczce akt.

PROCEDURA 8

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 8	Wniosek o udostępnienie danych osobowych na podstawie przepisów prawa	**Nr wersji procedury : 1.0**
		Ilość stron : 5

....., dnia .....

Sz.P.....
.....

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1.Wnioskodawca :

2. Podstawa prawna upoważniająca do pozyskania informacji :

3.Oznaczenie lub nazwa zbioru, z którego mają być udostępnione informacje:

4.Zakres żądanych informacji ze zbioru:

5.Forma przekazania lub udostępnienia informacji:

6.Imię, nazwisko osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią:

.....
(Imię i nazwisko, podpis)

Opinia Inspektora Ochrony Danych Osobowych :

.....
(Podpis IODO)

Decyzja Administratora danych :

.....
(Podpis Administratora danych)

Załącznik nr 14

PROCEDURA ZWIĄZANA Z ZABEZPIECZENIEM KOMPUTERÓW

Procedura bezpieczeństwa przetwarzania danych osobowych		Data wprowadzenia: 00.00.2018 r.
Numer Procedury : 9	PROCEDURA ZWIĄZANA Z ZABEZPIECZENIEM KOMPUTERÓW	**Nr wersji procedury : 1.0**
		Ilość stron : 5

1. CEL
   Celem niniejszej Instrukcji jest określenie zasad obsługi komputerów w zakresie bezpieczeństwa fizycznego oraz bezpieczeństwa informacji podlegających ochronie u Administratora.
2. ZAKRES STOSOWANIA
   Instrukcja przeznaczona jest do stosowania przez wszystkich pracowników Administratora posiadających w swoim wyposażeniu komputery stacjonarne lub przenośne.
3. POSTĘPOWANIE

3.1 Postanowienia ogólne

3.1.1. Pracownicy Administratora przy realizacji prac służbowych korzystają z komputerów stacjonarnych lub przenośnych

3.1.2. Administrator powierza pracownikowi komputer na podstawie pisemnego protokołu przekazania, zawierającego:

- typ i model komputera;
- specyfikację elementów zestawu (w zależności czy przekazany jest komputer przenośny czy stacjonarny): komputer, monitor, klawiatura, myszka, zewnętrzne napędy nośników, karty rozszerzeń, kable, torba, itp.
- numery seryjne komputera, elementów dodatkowych zestawu, numery licencji zainstalowanego oprogramowania
- specyfikację zainstalowanego oprogramowania systemowego, użytkowego i narzędziowego

3.1.3. Z komputera przenośnego do celów służbowych może korzystać wyłącznik pracownik, któremu został przyznany w ramach przydziału

3.1.4. Instalacji i konfiguracji systemu operacyjnego, oprogramowania użytkowego i narzędziowego oraz zmian w konfiguracji komputera może dokonywać wyłącznie Administrator Systemu Informatycznego (ASI) lub wyznaczona przez niego osoba.

3.1.5. ASI lub wyznaczona przez niego osoba zobowiązany jest do zainstalowania na komputerze najnowszych poprawek dotyczących bezpieczeństwa systemu operacyjnego

3.1.6. ASI określa liczbę kont oraz grup użytkowników zdefiniowanych w lokalnej bazie użytkowników systemu operacyjnego komputera, która powinna być ograniczona do niezbędnego minimum. Nieużywane konta wyłącza lub usuwa, a pozostałym nadaje możliwie ograniczone uprawnienia.

3.1.7. Konto użytkownika nie powinno mieć uprawnień równoważnych uprawnieniom Administratora. Jeśli w systemie operacyjnym zostało zdefiniowane zostało konto Administratora, użytkownik nie powinien mieć do niego dostępu.

3.2. Blokada dostępu do systemu operacyjnego

3.2.1. Komputery użytkowane przez pracowników, na których przetwarza się informacje chronione muszą mieć założone zabezpieczenia przed nieautoryzowanym uruchomieniem systemu operacyjnego. Takim zabezpieczeniem są hasła zdefiniowane przez ASI.

3.3. Ochrona podczas używania komputera

3.3.1. W komputerze powinien być uaktywniony wygaszacz ekranu chroniony hasłem. Konfiguracja komputera przenośnego powinna zapewniać przejście w stan uśpienia czy hibernacji po czasowym nieużywanie komputera. Ponowne uruchomienia komputera z takiego stanu wymaga podania identyfikatora i hasła użytkownika.

Uwaga 1. Czas bezczynności komputera, po którym wyłącza się wygaszacz ekranu nie powinien być dłuższy niż 10 minut

Uwaga 2. W przypadku komputerów przenośnych, użytkownik powinien dodatkowo zabezpieczyć komputer przed nieupoważnionym dostępem osób trzecich, kradzieżą, itp.

3.4. Ochrona podczas transportu

3.4.1. Użytkownik ma obowiązek zapewnić/zadbać, aby w czasie transportu komputer przenośny był wyłączony, ewentualnie znajdował się w stanie hibernacji

3.4.2 Komputer przenośny powinien być transportowany w oryginalnym etui lub walizce chroniącej go przed uszkodzeniem

Uwaga 1. Użytkownik komputera przenośnego, służącego do przetworzenia informacji chronionych, w szczególności danych osobowych, obowiązany jest do zachowania szczególności danych osobowych, zobowiązany jest do zachowania szczególnej ostrożności podczas transportu i zabezpieczenia tego komputera poza obszarem przetwarzania w taki sposób, aby uniemożliwić dostęp do tych informacji osobie niepowołanej. Użytkownik nie powinien zezwalać osobom nieupoważnionym na korzystanie z komputera.

3.5 Zabezpieczenia antywirusowe

3.5.1. Na komputerze musi być zainstalowany program antywirusowy

3.5.2. Program antywirusowy powinien automatycznie aktualizować bazy antywirusowe.

3.6 Postępowanie w razie kradzieży lub zagubienia

3.6.1. Po zaginięciu lub kradzieży komputera należy niezwłocznie zgłosić ten fakt do ASI.

3.7 Postanowienia końcowe

3.7.1. Osoby korzystające z komputerów zobowiązane są do zapoznania się z treścią niniejszej *Instrukcji* i przestrzegania postanowień w niej zawartych oraz założenia oświadczenia dotyczącego znajomości jej treści

Załącznik nr 15– Procedura związana z usunięciem nośników

1. Pod pojęciem nośnik informatyczny rozumiemy:
a) Dyski twarde komputerowe i serwerowe wszelkich typów.
b) Płyty CD, DVD lub podobne.
c) Taśmy magnetyczne.
d) Pamięci flash (pendrive).
e) Dyski przenośne HDD, SSD itp.
2. Procedura wycofywania dotyczy nośników zawierających informacje poufne (w tym dane osobowe) lub oprogramowanie podlegające licencjonowaniu.
3. Wycofaniu podlegają te nośniki, dla których minął okres ich ważności, nie przewiduje się ich dalszego użytkowania lub istnieje prawdopodobieństwo, że dalsze ich użytkowanie może nie spełniać wymogów bezpieczeństwa przechowywania informacji.
4. Poprzez niszczenie danych, zapisanych na nośniku, rozumieć należy takie ich zniszczenie, które uniemożliwia ponowne ich odtworzenie. Zniszczenie danych może wykorzystywać metody zarówno programowe (użycie programów do kasowania danych) jak i sprzętowe (fizyczne zniszczenie nośnika).
5. Dopuszcza się składowanie nośników przeznaczonych do wycofania, stosując następujące zasady:
a) nośniki muszą być przechowywane w metalowym sejfie, w zamykanym pomieszczeniu, do którego nie mają dostępu osoby trzecie;
b) nośniki przeznaczone do wycofania muszą być odpowiednio oznaczone, w sposób uniemożliwiający ich przypadkowe, ponowne użycie;
6. Niszczenia nośników dokonuje się w następujący sposób:
a) Dyski twarde, dyski SSD, pamięci przenośne typu flash (w tym pendrive, dyski przenośnie), taśmy magnetyczne należy przekazać ASI Administratora. Po ocenie przez ASI stanu technicznego nośnika podejmuje on decyzję o sposobie usunięcia z niego danych:
i. jeżeli nośnik nie jest uszkodzony, usunięcie danych następuje przy wykorzystaniu specjalnie do tego celu przeznaczonych programów;
ii. w przypadku gdy nie można usunąć danych z nośnika w sposób programowy, należy go przekazać do fizycznego zniszczenia wyspecjalizowanej firmie, zajmującej się profesjonalnym niszczeniem danych;
b) Płyty CD, DVD itp. przełamuje się na kilka części, lub niszczy w niszczarce przeznaczonej do utylizacji płyt CD.
7. Po zakończeniu niszczenia, należy sporządzić odpowiedni protokół likwidacyjny nośników. Protokół musi zawierać wyszczególnienie zniszczonych nośników wraz z ich opisem, datą likwidacji, nazwiska osób, które tego dokonały, lub raport z firmy, której nośniki zostały przekazane do zniszczenia.
8. W **Rejestrze Wycofanych Nośników** należy odnotować fakt wycofania nośników, dołączając protokół likwidacyjny.
9. Wzór protokołu likwidacyjnego nośników stanowi Załącznik nr 1.

Załącznik nr 1 do „Procedury wycofywania nośników"

Miejscowość, data

.....
/pieczęć/

PROTOKÓŁ LIKWIDACYJNY NOŚNIKÓW INFORMATYCZNYCH

Komisja w składzie:
1. Przewodniczący komisji: .....
2. Członek komisji: .....
3. Członek komisji: .....

potwierdza zniszczenie następujących nośników informatycznych:

L.p.	Opis nośnika	Data likwidacji	Osoba odpowiedzialna za zniszczenie nośnika
1.	Dysk twardy .....,	03.03.2017	Np. Jan Kowalski
2.	Pamięć flash (pendrvie).....	03.03.2017	Np.Jan Kowalski
3.	Dysk SSD	09.04.2017	Np.Andrzej Nowak
...			

Podpisy członków komisji:

1. .....
2. .....
3. .....

Załącznik nr 16 - Polityka Zarządzania Ryzykiem w procesach przetwarzania danych osobowych w Urzędzie Miasta i Gminy Mikołajki

Rozdział 1
Postanowienia ogólne

§ 1. Ilekroć w dokumencie jest mowa o:

1) **administratorze danych** – należy przez to rozumieć Gminę Mikołajki, z siedzibą przy ul. Kolejowej 7, 11-730 Mikołajki, reprezentowaną przez Burmistrza Miasta Mikołajki.

2) **proces przetwarzania danych** – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych w celu określonego celu przetwarzania;

3) **operacji przetwarzania danych** – należy przez to rozumieć każdą czynność wykonywaną na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka, jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawniane poprzez wysłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

4) **ryzyku** – należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów w zakresie ochrony danych osobowych. Ryzyko mierzone jest siłą skutku oddziaływania oraz prawdopodobieństwem jego wystąpienia;

5) **zarządzanie ryzykiem** – należy przez to rozumieć realizowany przez administratora danych osobowych proces, którego celem jest identyfikacja potencjalnych ryzyk, które mogą mieć wpływ na realizację celów i zadań jednostki;

6) **ocena ryzyka** – należy przez to rozumieć czynność polegającą na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie projektowania systemu bezpieczeństwa danych;

7) **kryteriach akceptacji ryzyka** – są to kryteria, które określają dopuszczalność ryzyka, zdefiniowane poprzez wartość progową.

8) **rejestr ryzyk** – należy przez to rozumieć dokument odzwierciedlający przeprowadzoną identyfikację i analizę ryzyk, a także przyjętą reakcję na ryzyko;

9) **bezpieczeństwie informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

10) **zdarzeniu związanym z bezpieczeństwem danych** – zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem danych;

11) **incydencie** związanym z bezpieczeństwem danych – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne zakłócenia zadań i zagrażają bezpieczeństwu danych;

12) **zagrożeniu** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;

13) **podatność** – słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki;

14) **dostępności** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;

15) **integralności** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;

16) **poufności** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;

§2. Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
§3. Polityka zarządzania ryzykiem w zakresie ochrony danych osobowych, zwana dalej „polityką zarządzania ryzykiem", obejmuje:
1) zakres zadań i obowiązków podmiotów uczestniczących w procesie zarządzania ryzykiem;
2) zasady i tryb identyfikacji ryzyka;
3) zasady i tryb dokonywania analizy ryzyka;
4) zasady określania właściwej reakcji na ryzyko.
§4. Polityka zarządzania ryzykiem ma zastosowanie dla wszystkich samodzielnych stanowisk.
§5. Zarządzanie ryzykiem jest procesem ciągłym i nie ogranicza się do działań określonych w §2.
§6. Celem zarządzania ryzykiem jest zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań w zakresie ochrony danych osobowych, poprzez ograniczenie prawdopodobieństwa wystąpienia ryzyka oraz zabezpieczanie się przed jego skutkami. Następuje to poprzez:
1) identyfikację zasobów służących do przetwarzania danych osobowych- załącznik nr 1,
2) rozpoznanie – czyli identyfikowanie ryzyka oraz zagrożeń, określenie rodzajów ryzyk i zagrożeń, które wiążą się z działalnością jednostki w zakresie ochrony danych osobowych i dokonywanie ich pomiaru;
3) ocenę ryzyka i prawdopodobieństwa wystąpienia zagrożenia i jego istotności, przy pomocy skali określonej w § 9.2;
4) zarządzanie ryzykiem, które polega na badaniu efektywności i skuteczności podejmowanych działań, poprzez system kontroli instytucjonalnej i zewnętrznej;
5) kontrolę zarządzania ryzykiem, której istotą podjętych działań jest ocena zastosowanych metod redukcji ryzyka, prowadząca do skutecznego i efektywnego realizowania celów i nałożonych zadań.

Rozdział 2
Zakresy zadań i obowiązków

§7. Za realizację polityki zarządzania ryzykiem odpowiada Administrator poprzez:
1) wyznaczanie osób odpowiedzialnych za kształtowanie i wdrażanie polityki zarządzania ryzykiem;
2) nadzór i monitorowanie skuteczności procesu zarządzania ryzykiem;
3) wyznaczanie poziomu akceptowalnego dla każdego ryzyka;
4) podejmowanie decyzji dotyczących sposobu reakcji na poszczególne ryzyka.
§ 7. 1. Pracownicy na samodzielnych stanowiskach odpowiadają za zarządzanie ryzykiem poprzez:
1) identyfikację ryzyk związanych z realizacją przydzielonych zadań w zakresie ochrony danych osobowych;
2) wskazywanie właścicieli zidentyfikowanych ryzyk;
3) przeprowadzanie analizy zidentyfikowanego ryzyka we współpracy z IOD;
4) proponowanie sposobu postępowania w odniesieniu do poszczególnych ryzyk;
5) wdrażanie działań zaradczych w stosunku do zidentyfikowanego ryzyka.
§ 7. 2. Pracownicy wymienieni w §7 ust. 1 są zobowiązani do współpracy Administratorem Danych oraz Inspektorem Ochrony Danych.

Rozdział 3
Identyfikacja ryzyka

§8. Identyfikacja ryzyk prowadzona jest dla wszystkich procesów w związku, z którymi przetwarzane są dane osobowe, na poziomie jednostki i na poziomie poszczególnych samodzielnych stanowisk pracy.

§8.1. W procesie identyfikacji ryzyka uwzględnia się zagrożenia. Ze względu na ich źródło ryzyka dzielą się na:

1) zewnętrzne – rodzaj ryzyka determinowanego przez czynniki zewnętrzne;
2) wewnętrzne – ryzyko to obejmuje działania wewnętrzne placówki i może być zarządzane wewnątrz jednostki.

§8.2 Każdy pracownik ma prawo i obowiązek zgłaszania swojemu bezpośredniemu przełożonemu ryzyk zidentyfikowanych podczas wykonywania przydzielonych zadań w zakresie ochrony danych osobowych.

Rozdział 4
Analiza ryzyka

§9. Każde ryzyko w zakresie ochrony danych osobowych podlega analizie pod kątem jego istotności na osiąganie celów i zadań. Istotność ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków.

§9.1. Każde ryzyko jest oceniane pod względem prawdopodobieństwa jego wystąpienia i skutku oddziaływania.

§9.2. Przy ocenie prawdopodobnych skutków wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 4, gdzie;

1) 1- oznacza niewielki skutek
2) 2 – oznacza znaczący skutek
3) 3 – oznacza bardzo znaczący skutek
4) 4 – oznacza skutek katastrofalny

§9.3. Przy ocenie prawdopodobieństwa wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 3, gdzie:

1) 1 – oznacza bardzo niskie prawdopodobieństwo, zdarzenie na przestrzeni funkcjonowania Urzędu nie wystąpiło
2) 2 – oznacza małe prawdopodobieństwo zdarzenie nie wystąpiło w okresie 12 miesięcy poprzedzających dzień sporządzenia analizy, lecz miało miejsce w historii funkcjonowania Urzędu,
3) 3 – oznacza duże prawdopodobieństwo, że zdarzenie nastąpiło w okresie 12 miesięcy poprzedzających dzień sporządzenia analizy i istnieje duże prawdopodobieństwo jego wystąpienia ponownego

§9.4. Przy ocenie skali ryzyka przyjmuje się skalę punktową od 1 do 12, gdzie:

1) 1-3- oznacza niskie ryzyko
2) 4-6- oznacza średnie ryzyko
3) 7-12- oznacza bardzo wysokie ryzyko

§9.5. Wynik ryzyka powstaje poprzez iloczyn punktów prawdopodobieństwa wystąpienia oraz punktów znaczenia skutku wystąpienia zagrożenia.

Rozdział 5
Reakcja na ryzyko

§10. Dla każdego istotnego zidentyfikowanego ryzyka właściciel ryzyka wskazuje optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

1) tolerowanie – będzie to miało miejsce w przypadkach, kiedy koszty skutecznego przeciwdziałania ryzyku mogą przekraczać jego potencjalne korzyści, z zdolności do skutecznego przeciwdziałania są ograniczone lub wykraczające poza decyzje i działania wewnętrzne;
2) przeniesienie – dotyczyć to będzie kategorii ryzyk w odniesieniu do których nastąpi przeniesienie ich na inna instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług na zewnątrz;
3) wycofanie się – dotyczyć to będzie grypy ryzyk dla których mimo podejmowanych działań nie udało się zmniejszyć ich istotności do akceptowanego poziomu;

4) przeciwdziałanie – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań prowadzących do ich likwidacji, lub znacznego ograniczenia.

Rozdział 6
Ocena skutków dla ochrony danych (DPIA)

§11. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii- ze względu na swój charakter, kontekst i cele z dużym prawdopodobieństwem może spowodować wysokie naruszenie prawa i wolności osób fizycznych, ADO w porozumienie z IOD i ASI przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem przeprowadza się pojedynczą ocenę.

§11.1. Ocena opiera się w szczególności na ocenie:

a) czy przetwarzane dane podlegają profilowaniu,
b) czy przetwarzanie danych obejmuje automatyczne podejmowanie decyzji, które wywierają znaczący wpływ na prawa osoby, której dane dotyczą,
c) czy wykonywany jest systematyczny monitoring na dużą skalę miejsc dostępnych publicznie,
d) czy przetwarzane są dane szczególnych kategorii o których mowa w art. 9 i 10 Rozporządzenia lub dane dotyczące wyroków skazujących, naruszeń prawa, lub związanych z tym środków bezpieczeństwa,
e) czy zbiory danych podlegają łączeniu,
f) czy dane osobowe są przetwarzane z wykorzystaniem innowacyjnych technologii lub z wykorzystaniem innowacyjnych środków organizacyjnych, w szczególności dotyczących identyfikacji osób fizycznych z zastosowaniem linii papilarnych lub z wykorzystaniem biometrii,
g) czy dane są przekazywane poza UE,
h) czy dane są przetwarzane na wielką skalę,
i) czy operacje przetwarzania utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw.

Rozdział 7
Postanowienia końcowe

§12. Analizę ryzyka przeprowadza się cyklicznie, nie rzadziej jednak niż raz na rok.

Załącznik nr 1 do polityki Zarządzania Ryzykiem

SPRZĘT I OPROGRAMOWANIE
Zagrożenie:

a. Pożar
b. Zniszczenie danych/ Zniszczenie urządzeń lub nośników danych
c. Utrata na skutek zjawisk starzenia się nośników danych (kurz, butwienie itp.)
d. Zalanie
e. Zjawiska pogodowe/ zawalenie budynku/ zapadnięcie ziemii
f. Powódź
g. Inne zjawiska o charakterze katastroficznym
h. Awaria systemu klimatyzacji
i. Utrata dostaw energii elektrycznej
j. Brak dostaw usług telekomunikacyjnych
k. Ujawnione próby pozyskania danych osobowych z wykorzystaniem technik kwalifikowanych, jako szpiegowanie (np. w sieci lub na terenie jednostki)
l. Podsłuch
m. Kradzież nośników danych lub dokumentów
n. Składanie wniosków w trybie dostępu do informacji publicznej
o. Próby pozyskiwania informacji przez osoby trzecie o miejscu i sposobie przechowywania danych
p. Posługiwanie się nielicencjonowanym, sfałszowanym oprogramowaniem
q. Kradzież urządzeń służących przetwarzaniu danych
r. Niezamierzone ujawnienie danych
s. Używanie nośników niebędących własnością jednostki
t. Odtwarzanie danych z nośników przeznaczonych do zniszczenia
u. Awaria urządzenia służącego przetwarzaniu danych (jednostki, komputerowe, skanery, druki)
v. Niewłaściwe funkcjonowanie urządzeń służących przetwarzaniu danych (komputery, drukarki, skanery)
w. Przeciążenie systemów informatycznych skutkujące zawieszeniem pracy
x. Niewłaściwe fuknojonowanie systemów informatycznych
y. Naruszenie zdolności utrzymania systemu informatycznego (brak przedłużenia licencji, brak dostępu do aktualizacji, brak dostępu do wsparcia serwisowego)
z. Użycie urządzeń przez nieuprawnionego użytkownika
aa. Przetwarzanie danych przez osobę nieupoważnioną
bb. Korzystanie z usług przypadkowch serwisantów
cc. Nieuprawnione, nieuzasadnione kopiowanie danych
dd. Błąd użytkownika- działanie lub próba podjęcia działań niezgdonych z przyjętymi zasadami bezpieczeństwa
ee. Fałszowanie uprawnień, przetwarzanie danych z wykorzystaniem hasła dostępi, loginu innej osoby
ff. Brak dostępności personelu posiadającego uprawnienia
gg. Brak odebrania uprcowników, którzy na skutek odejścia, zmiany wydziału przestali przetwarzać dane

Zabezpieczenia:

a. pliki/foldery plików zawierające dane osobowe zabezpieczone są hasłem. Hasło jest znane wyłącznie osobom upoważnionym do przetwarzania danych zawartych w pliku/folderze; zachowanie szczególnej ostrożności przy zapisywaniu plików/folderów na dysku wspólnym
b. pracownicy nie mają możliwości samodzielnej instalacji programów/oprogramowania
c. zainstalowanie i regularna aktualizacja oprogramowania antywirusowego
d. w przypadku konieczności przekazania sprzętu komputerowego do naprawy poza siedzibę Biblioteki/wymiany sprzętu na nowy – zagwarantowanie, że wszelkie użytkowane nośniki danych pozostają w siedzibie Biblioteki
e. komputery znajdują się w bezpiecznej odległości od okien (brak ryzyka zalania) i źródeł ciepła

f. kubki/szklanki z napojami, jedzeniem znajdują się w bezpiecznej odległości od sprzętu komputerowego

PRACOWNICY

Zagrożenia:

a. Utrata danych osobowych, zagubienie dokumentów
b. Niezgodne z prawem lub nieuprawnione zniszczenie
c. Nieuprawnione ujawnienie danych osobowych
d. Niedozwolone lub niezgodne z prawem przetwarzanie
e. Bezprawne przekazanie lub upublicznienie danych
f. Naruszenie prawa i procedur
g. Brak dyskrecji osób upoważnionych do przetwarzania danych osobowych
h. Celowe lub przypadkowe uszkodzenie, zniszczenie lub nieprawidłowa modyfikacja danych
i. Utrata kluczy do pomieszczeń, w których przetwarzane są dane osobowe
j. Nieprzestrzeganie zasady „czystego biurka"
k. Pozostawianie dokumentu zawierającego dane osobowe w miejscu nienadzorowanym

Zabezpieczenia i środki zaradcze:

a. Dopuszczenie do przetwarzania danych dopiero po otrzymaniu przez nich upoważnień do przetwarzania danych osobowych
b. Regularne szkolenia pracowników, na których w sposób wyczerpujący omówione są zagadnienia związane z ochroną danych osobowych
c. Szkolenia dla nowoprzyjętych pracowników przed podjęciem pracy bądź w pierwszych jej dniach
d. Zamykanie na klucz pomieszczeń, w których przetwarzane są dane osobowe w razie konieczności ich opuszczenia
e. Niepozostawianie kluczy od pomieszczeń w drzwiach
f. Obowiązkowe blokowanie komputera przy zamiarze opuszczenia stanowiska pracy
g. Zamykanie dokumentów zawierających dane osobowe na klucz
h. Niepozostawianie osób nieuprawnionych samych w pomieszczeniach na dłuższy okres pozwalając na nieuprawniony wgląd do danych
i. Zakaz bądź ograniczenie możliwości wynoszenia danych osobowych poza obszary przetwarzania danych osobowych
j. Zachowywanie dyskrecji przy udzielaniu informacji
k. Zachowanie należytej staranności i ostrożności podczas przetwarzania danych osobowych

SIEDZIBA

Zagrożenia:

a. słaby zamek oraz drzwi wejściowe
b. brak systemu alarmowego oraz monitoringu kamer
c. zbyt słabe zabezpieczenia fizyczne i techniczne przed kradzieżą
d. brak odpowiednich zabezpieczeń fizycznych
e. niedostateczna ochrona p-poż
f. brak wydzielonego pomieszczenia służącego do archiwowania danych
g. dokumenty bieżące przechowywane są w jednej szafie z dokumentami archiwalnymi

Zabezpieczenia:

a. kraty w oknach
b. dokumenty zawierające dane osobowe zamykane są w szafach na klucz
c. pomieszczenia, w których przechowywane są dane osobowe zamykane są co najmniej na klucz
d. w budynku zapewniono sprawny sprzęt gaśniczy
e. pracownicy są zaznajomieni z zasadami postępowania w przypadku ewakuacji

ORGANIZACJA

Zagrożenia:

a. brak nadzoru nad pracownikiem
b. brak regularnych przeglądów pod kątem ograniczenia czasowego realizowanych przez ADO

Zabezpieczenia:

a. opracowanie procedur związanych z ochroną danych, które są precyzyjne i napisane zrozumiałym językiem
b. wprowadzenie zabezpieczeń/procedur dot. potwierdzania tożsamości osób, którym udzielany jest dostęp do danych osobowych (np. do danych przechowywanych w archiwum)
c. okresowy przegląd przechowywanych danych osobowych (w tym danych przechowywanych w archiwum) w celu umożliwienia podjęcia decyzji o ich zniszczeniu (zakończenie obowiązkowego okresu przechowywania danych)
d. wyznaczenie Inspektora Ochrony Danych
e. przeprowadzanie audytów zgodności z przepisami

Załącznik nr 2 do Zarządzenia Burmistrza Miasta Mikołajki nr 138/2018 w sprawie wdrożenia Polityki Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Mikołajkach

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM			
URZĄD MIASTA i GMINY W MIKOŁAJKACH ul. Kolejowa 7 11-730 Mikołajki	Strona/ stron	20	
Cel dokumentu: Określenie zasad bezpiecznej pracy w systemach informatycznych służących do przetwarzania danych osobowych.	Wersja: Z dnia:	1.0 **28.12..2018**	
Odpowiedzialny:	**Burmistrz**	**Stosowanie:**	**Wszystkie stanowiska pracy**

Spis treści