Załącznik nr 1 do Zarządzenia nr 76/2018
Burmistrza Miasta Kowalewo Pomorskie
z dnia 25.05.2018r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

dla Urzędu Miejskiego w Kowalewie Pomorskim.

Kowalewo Pomorskie 25.05.2018r.

SPIS TREŚCI

1. **Informacje ogólne:**

Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Urzędu Miejskiego w Kowalewie Pomorskim jako Administratora Danych Osobowych z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

1. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
2. ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
3. rozporządzenia (akty wykonawcze), które będą wydawane do ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
4. przepisy sektorowe (przepisy prawa materialnego): np. Kodeks pracy, Prawo telekomunikacyjne, Prawo bankowe, ustawa o działalności ubezpieczeniowej i reasekuracyjnej, ustawa o swobodzie działalności gospodarczej.

DEFINICJE

RODO – Rozporządzenie PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r.
POLITYKA- Polityka Bezpieczeństwa Danych Osobowych dla Urzędu Miejskiego w Kowalewie Pomorskim
URZĄD- Urząd Miejski w Kowalewie Pomorskim
ADO- ADMINISTRATOR DANYCH OSOBOWYCH- - Burmistrz Miasta Kowalewo Pomorskie
IODO- Inspektor Ochrony Danych Osobowych – osoba powołana przez ADO do nadzorowania przestrzegania zasad ochrony danych osobowych w Urzędzie
Administrator Zbioru- osoba- kierownik lub samodzielne stanowisko pracy, odpowiedzialna za gromadzenie danych osobowych, tworzenie Rejestrów Czynności Przetwarzania Danych Osobowych
Użytkownik zbioru- osoba (pracownik) posiadająca upoważnienie do działania na zbiorze danych osobowych.
Informatyk- osoba w Urzędzie zajmująca się zabezpieczeniem systemów teleinformatycznych i konserwacją urządzeń do przetwarzania danych
Dane Osobowe- informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
Przetwarzanie- operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczenie, usuwanie lub niszczenie.

Zbiór danych- uporządkowany zestaw danych osobowych dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest scentralizowany, zdecentralizowany czy rozporoszony funkcjonalnie lub geograficznie (na różnych nośnikach).
Pseudonimizacja- przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub każdy inny podmiot, któremu ujawnia się dane osobowe. Nie zalicza się tu organów publicznych, które mogą otrzymać dane osobowe w ramach konkretnego postepowania zgodnie z prawem unijnym lub członkowskim np. organ podatkowy, skarbowy, celny.
Zgoda osoby, której dane dotyczą- dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych
Naruszenie ochrony danych osobowych- naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych

2. Cel i zakres Polityki Bezpieczeństwa

RODO nakłada na ADO obowiązek stosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę gromadzonych i przetwarzanych danych osobowych oraz zabezpieczenie ich między innymi przed udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem prawa, a także zmianą, utratą, uszkodzeniem lub zniszczeniem.
Celem niniejszej Polityki Bezpieczeństwa przetwarzania danych osobowych jest opracowanie optymalnych i zgodnych z wymogami prawa zasad przetwarzania danych, których zbieranie i przetwarzanie jest niezbędne dla realizacji zadań ustawowych Urzędu Miejskiego w Kowalewie Pomorskim.
Wykaz poszczególnych zbiorów danych osobowych stanowi **załącznik nr 1** do Polityki Bezpieczeństwa.
Dane osobowe we wskazanych powyżej zbiorach danych są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.

3. Obszar przetwarzania danych osobowych

W Urzędzie Miejskim w Kowalewie Pomorskim przetwarzane są dane osobowe w następujących lokalizacjach:
- Budynek Urzędu przy ul. Plac Wolności 1
- Budynek Urzędu przy ul. Św. Mikołaja 5
- Budynek Urzędu przy ul. Plac Wolności 3
- Budynek Urzędu- pływalnia przy ul. Jana Pawła II
- Budynek Urzędu- Centrum Rekreacji i Sportu przy ul. Chopina 28
- Budynek i plac targowiska przy ul. Strażackiej 1,

4. Obowiązki i odpowiedzialność

1. Do najważniejszych obowiązków **Administratora Danych Osobowych** należy:
1) Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych,
2) Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa,
3) Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
4) Zapewnienie szkoleń użytkowników przed dopuszczeniem do pracy na zbiorach i w systemach informatycznych przetwarzających dane osobowe,

5) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
6) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
7) Nadzór nad bezpieczeństwem danych osobowych,
8) Kontrola działań pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
9) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,

2. Do najważniejszych obowiązków **Informatyka** należy:
1) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2) Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
3) Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
4) Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
5) Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych w umowach serwisowych,
6) Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
7) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
8) Zmiana lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
9) Zarządzanie licencjami oraz procedurami ich dotyczącymi,
10) Prowadzenie profilaktyki antywirusowej.

3. Do najważniejszych obowiązków **Administratorów Zbiorów jak i Użytkowników Zbiorów** należy:
1) Posiadanie upoważnienia do zbioru danych osobowych
2) Znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do danych osobowych znajdujących się na stanowisku pracy,
3) Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami,
4) Zachowanie w tajemnicy danych osobowych, do których uzyskały dostęp oraz informacji o sposobach ich zabezpieczenia,
5) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
6) Informowanie ADO o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe,
7) Zapoznanie się z Polityką Bezpieczeństwa przetwarzania danych osobowych

5. Zarządzanie Ochroną Danych Osobowych

1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.
2. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.
3. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.
4. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

5. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
6. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.
7. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydawane przez ADO.
8. Każdy użytkownik przed dopuszczeniem do pracy na zbiorze danych w wersji elektronicznej lub papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych,
9. Za przeprowadzenie szkolenia odpowiada ADO.
10. Po zaznajomieniu się z zasadami ochrony danych osobowych Użytkownik Zbioru, przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania przez podpisanie oświadczenia użytkownika, który stanowi **załącznik nr 2** do Polityki Bezpieczeństwa.

6. Upoważnienia do przetwarzania danych osobowych oraz rejestr upoważnień.

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych. Wzór wniosku o wydanie upoważnienia oraz druk upoważnienia **załącznik nr 3** Polityki Bezpieczeństwa
2. W celu otrzymania przez pracownika Urzędu upoważnienia do zbiorów zawierających dane osobowe należy:
1) złożyć pisemny wniosek podpisany przez pracownika oraz Administratora Zbioru ze wskazaniem danych wnioskodawcy (imię, nazwisko, pesel, stanowisko pracy) wraz z nazwą zbioru danych osobowych do którego upoważnienie jest potrzebne.
2) dostarczyć do Administratora Danych podpisane oświadczenie użytkownika o zapoznaniu się z Polityką Bezpieczeństwa
3. Na podstawie otrzymanego oświadczenia ADO upoważnia Użytkownika do przetwarzania danych osobowych i wydaje pisemne upoważnienie do przetwarzania danych osobowych,
4. Upoważnienie, o którym mowa powyżej powinno zawierać dane osobowe Użytkownika, czas trwania, nazwy zbiorów danych osobowych.
5. Upoważnienie przechowywane powinno być na stanowisku pracy Użytkownika,
6. Użytkownik może posiadać jednocześnie kilka upoważnień do różnych zbiorów danych osobowych
7. Upoważnienie może być w każdym czasie pisemnie odwołane przez ADO.
8. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, w tym w szczególności wygaśnięcia stosunku pracy lub umowy cywilnoprawnej łączącej Użytkownika z ADO,
9. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miejskim w Kowalewie Pomorskim jest prowadzona przez ADO i **stanowi załącznik nr 4** do Polityki Bezpieczeństwa.

7. Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane na pisemny wniosek wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dane dotyczą.
2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą ADO.
3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
4. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

8. Dokonywanie obowiązku informacyjnego

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, należy poinformować tę osobę o tym fakcie stosując Klauzulę Informacyjną stanowiącą **załącznik nr 5** do Polityki Bezpieczeństwa

9. Przetwarzanie danych osobowych. Wymagania bezpieczeństwa.

1. Dane osobowe mogą być przetwarzane wyłącznie w obszarze przetwarzania danych osobowych, na które składają się pomieszczenia biurowe w budynkach urzędu wymienionych w pkt. 3. z wyjątkiem sytuacji udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych.
2. Dane osobowe w Urzędzie przetwarzane są przy zastosowaniu należytych i odpowiednich zabezpieczeń zapewniających ich ochronę w postaci wymienionych poniżej środków.

1). Środki organizacyjne:
- wdrożenie Polityki Bezpieczeństwa danych osobowych
- wdrożenie „Instrukcji określającej procedurę zabezpieczenia budynków Urzędu Miejskiego w Kowalewie Pomorskim i przechowywania kluczy”
- wdrożenie regulaminów Systemu Monitoringu

2) Środki techniczne:
- zbiory danych osobowych przetwarzane są wyłącznie na autoryzowanym sprzęcie służbowym,
- stacje robocze wyposażone są w indywidualną ochronę antywirusową,
- dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- ADO nie dopuszcza, a nawet zakazuje stosowania prywatnych nośników informacyjnych (pendrive) bez systemu zabezpieczającego (szyfrującego)
- zakazuje się zapisywania w lokalizacjach sieciowych informacji do których może mieć dostęp nieupoważniony do odczytania tej informacji pracownik, np. przy zapisywaniu informacji na „skrzynce” t.j. folderze dostępnym przez wszystkich pracowników zakładamy, że każdy z pracowników odczytał zapisaną informację.

3) Środki ochrony fizycznej:
- wszystkie pomieszczenia (biura), w których znajdują się zbiory danych osobowych, są zamykane na klucz, a dostęp do nich odbywa się wyłącznie w obecności pracowników,
- okna pomieszczeń na parterze są zabezpieczone kratami
- pomieszczenia przy ul. Chopina 28 i ul. Jana Pawła II, w którym przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy
- drzwi do obiektów posiadają podwójne zamki antywłamaniowe,

3. Użytkownicy zbiorów są zobowiązani do:
- zachowania tajemnicy danych
- strzeżenia akt, przenośnych pamięci, laptopów przed dostaniem się w niepowołane ręce
- ustawianie ekranów komputerów w sposób, aby wyświetlające się na nich dane nie były widoczne dla klientów,
- nieużywanie powtórnie zadrukowanych jednostronnie zbędnych pism i dokumentów
- niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe bez obecności osoby upoważnionej do przetwarzania danych osobowych,
- niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze
- używania tylko własnego hasła i identyfikatora,
- niepodłączania do listw podtrzymujących napięcie sprzętu komputerowego innych urządzeń (czajników, wentylatorów, ładowarek)
- opuszczenia stanowiska pracy dopiero po zaktywizowaniu się wygaszacza ekranu lub po innym zablokowaniu stacji roboczej

- kończenia pracy po prawidłowym wylogowaniu się z systemu i wyłączeniu komputera, odcięciu napięcia w UPS i na listwie
- wykonywania kopii roboczych w takiej częstotliwości, aby zapobiec ich utracie
- fizycznego niszczenia nośników danych, które nie będą więcej używane
- niszczenia w niszczarce lub chowania w szafie wszelkich wydruków zawierających chronione dane osobowe
- przestrzegania zasad „czystego biurka" oraz Instrukcji określającej procedurę postepowania z kluczami,
- niedopuszczenia do pracy pracownika podległego (stażysty, praktykanta) bez zapewnienia mu przeszkolenia z zakresu ochrony danych osobowych oraz otrzymania upoważnienia do pracy na zbiorze danych
- zachowania wyjątkowej ostrożności w czasie pracy na dokumentach zawierających dane osobowe poza miejscem pracy np. w czasie podróży służbowej, zebrania wiejskiego,

10. Sprawdzenie stanu systemu ochrony danych osobowych

1. ADO minimum raz w roku sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2. Okresowy przegląd Polityki Bezpieczeństwa powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Urzędu Miejskiego oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

11. Rejestr Czynności Przetwarzania Danych Osobowych

1. Administrator Danych prowadzi Rejestr czynności przetwarzania danych osobowych za które odpowiada,
2. Rejestr wskazuje Administratora danych, cele przetwarzania, opis kategorii osób i danych osobowych, kategorie odbiorców danych, terminy gromadzenia danych, oraz opis techniczny i organizacyjnych środków bezpieczeństwa.
3. Rejestr ma formę pisemną oraz elektroniczną i stanowi **Załącznik nr 6** do Polityki Bezpieczeństwa.

12. Procedura szacowania i zarządzania ryzykiem.

Celem Procedury jest określenie metodologii zarządzania ryzykiem w Urzędzie, metody tworzenia i utrzymania klasyfikacji informacji oraz oceny ryzyka. Stanowi ona **załącznik nr 7** do Polityki Bezpieczeństwa.

13. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych

1. Każdy Użytkownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym fakcie natychmiast poinformować ADO.
2. Czyni to wypełniając druk Zgłoszenia w sprawie naruszenia ochrony danych osobowych, będącego **Załącznikiem nr 8** do Polityki Bezpieczeństwa. Składa go w terminie nie późniejszym niż 72 godziny od stwierdzenia wystąpienia naruszenia,
3. W przypadku stwierdzenia wystąpienia zagrożenia, ADO prowadzi postępowanie wyjaśniające w toku którego:

1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
2) informuje o tym fakcie IODO
3) Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
4) Zabezpiecza ewentualne dowody;
5) Ustala osoby odpowiedzialne za naruszenie;
6) Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
7) Inicjuje działania dyscyplinarne;

8) Wyciąga wnioski i rekomenduje działania korygujące oraz prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości;
9) Prowadzi Rejestr naruszeń ochrony danych osobowych, który jest **Załącznikiem nr 9** do Polityki Bezpieczeństwa.

14. Postanowienia końcowe.

1. Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach funkcjonowania Urzędu Miejskiego w Kowalewie Pomorskim, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. ADO ma obowiązek zapoznać z treścią Polityki każdego Użytkownika.
3. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
6. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z RODO oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO.

Załącznik nr 1- Wykaz zbiorów danych osobowych
Załącznik nr 2- Druk oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa,
Załącznik nr 3- Druk wniosku o wydanie upoważnienia oraz druk upoważnienia
Załącznik nr 4 - Ewidencja osób upoważnionych do zbiorów danych osobowych
Załącznik nr 5- Klauzula Informacyjna
Załącznik nr 6- Rejestr czynności przetwarzania danych osobowych
Załącznik nr 7- Procedura szacowania i zarządzania ryzykiem.
Załącznik nr 8- Zgłoszenie w sprawie naruszenia ochrony danych osobowych
Załącznik nr 9- Rejestr naruszeń ochrony danych osobowych

Załącznik nr 1
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

Wykaz zbiorów danych osobowych Urzędu Miejskiego w Kowalewie Pomorskim.

L.p	Nazwa zbioru
1.	Dokumentacja wypadków przy pracy
2.	Dokumentacja szkoleń pracowników Urzędu Miejskiego
3.	Dokumentacja badań lekarskich pracowników Urzędu Miejskiego
4.	Oświadczenia majątkowe radnych
5.	Protokoły z posiedzeń Komisji
6.	Sprawy osobowe radnych gminy
7.	Reklamowanie osób od obowiązku pełnieia czynnej służby wojskowej w czasie ogłoszenia mob ilizacji i czasie wojny
8.	Wnioski i postulaty mieszkańców
9.	Zasiłki i pożyczki w celu ekonomicznego usamodzielnienia
10.	Wnioski i interpelacje radnych
11.	Sesje rady gminy
12.	Skargi i wnioski (rejestr)
13.	Rejestracja aktów urodzeń, małżeństw, zgonów
14.	Unieważnienie, sprostowanie, ustalenie treści, odtworzenie i uzupełnienie aktu stanu cywilnego
15.	Wpisywanie akt stanu cywilnego sporządzonych za granicą do polskich ksiąg
16.	Zezwolenie na zawarcie małżeństwa przed upływem miesiąca
17.	Zmiany imion i nazwisk
18.	Nadawanie medalu za długoletnie pożycie małżeńskie
19.	Nadawanie medalu dla rodziców za zasługi dla obronności kraju
20.	Zaświadczenia o zdolności do zawarcia małżeństwa za granicą
21.	Odpisy zupełne, skrócone i wielojęzyczne aktów stanu cywilnego
22.	Powiadamianie innych podmiotów i jednostek organizacyjnych o zmianach w aktach stanu cywilnego
23.	Udostępnianie innych informacji na podstawie akt stanu cywilnego
24.	Profilaktyka i konserwacja akt stanu cywilnego
25.	Sprawy konsularne
26.	Zgromadzenia i imprezy masowe
27.	Zbiórki publiczne
28.	Obywatelstwo
29.	Ewidencja ludności
30.	Aktualizowanie danych z ewidencji ludności
31.	Sprawy meldunkowe
32.	Udostępnianie danych i wydawanie zaświadczeń z ewidencji ludności lub dokumentacji wydanych dowodów osobistych
33.	Prowadzenie i obsługa rejestru wyborców
34.	Spis wyborców
35.	Udostępnianie danych z rejestru i spisu wyborców
36.	Organizacja kwalifikacji wojskowej
37.	Nakładanie obowiązku świadczeń osobistych na rzecz obronności i ich wykonywanie
38.	Przeznaczenie nieruchomości i rzecz ruchomych na cele świadczeń na rzecz obronności oraz wykonanie tych świadczeń
39.	Obsługa dowodów osobistych
40.	Planowanie w zakresie spraw obronnych
41.	Organizowanie systemu kierowania obronnością
42.	Przygotowanie publicznej i niepublicznej służby zdrowia na potrzeby obronne państwa
43.	Ewidencja osób otrzymujących dofinansowanie na usuwanie azbestu
44.	Rejestr zezwoleń na wycinkę drzew i krzewów
45.	Krajowy transport drogowy
46.	Rejestr zezwoleń na sprzedaż alkoholu
47.	Skargi i wnioski załatwiane bezpośrednio (w tym o wynajem pływalni)
48.	Szkolenia pracowników , badania własne bhp,
49.	Ewidencja podatników podatku rolnego
50.	Ewidencja podatników podatków lokalnych

51.	Zbiór odroczeń, umorzeń podatników
52.	Ewidencja wysłanych upomnień dot. zaległości podatkowych
53.	Wynagrodzenia pracowników placówek oświatowych oraz urzędu miejskiego
54.	Staże, praktyki, wolontariat
55.	Prace społecznie-użyteczne
56.	Nagrody dla nauczycieli i dyrektorów za ich osiągnięcia dydaktyczno wychowawcze
57.	Konkursy na stanowiska w urzędach
58.	Zapotrzebowanie i nabór do pracy
59.	Odznaczenia państwowe
60.	Konkursy w jednostkach podległych
61.	Oświadczenia majątkowe pracowników urzędu gminy i jednostek organizacyjnych.
62.	Kadry w Urzędzie
63.	Reklamowanie od służby wojskowej
64.	Rejestr korespondencji wychodzącej
65.	Młodociani pracownicy i ich pracodawcy
66.	Osoby nieubezpieczone ubiegające się o świadczenia opieki zdrowotnej finansowane ze środków publicznych
67.	Rejestr osób wpisanych do systemu sms
68.	Rejestr słuchaczy Uniwersytetu Trzeciego Wieku
69.	Obowiązek nauki
70.	Awans zawodowy nauczyciela na stopień nauczyciela mianowanego
71.	Projekt „EU-geniusz w naukowym labiryncie”
72.	Stypendia i nagrody w ramach „Długofalowego programu rozwoju oświaty”
73.	Rejestr sołtysów sołectw
74.	Zebrania wiejskie, zebrania wiejskie wyborcze
75.	Korespondencja przychodząca
76.	Korespondencja przychodząca – EPUAP
77.	Potwierdzenie profilu zaufanego – EPUAP
78.	Rejestr skarg i wniosków
79.	Rejestr wniosków o udostępnienie inf. Publicznej
80.	Archiwum zakładowe
81.	Rejestr wniosków o przyznanie stypendium i zasiłku szkolnego
82.	Arkusze Organizacji prowadzonych przez gminę szkół i przedszkola
83.	Wnioski o gadżety promocyjne
84.	Rejestr wniosków o przyznanie stypendium za wysokie wyniki w nauce
85.	Rejestr wniosków o działania promocyjne na rzecz gminy
86.	Rejestr wniosków – dowóz uczniów do szkół
87.	Rozgraniczenia nieruchomości i wznawianie znaków granicznych
88.	Ewidencja miejscowości, ulic i adresów
89.	Opłaty adiacenckie z tyt. podziału i wybudowania urządzeń infrastruktury technicznej
90.	Numeracja porządkowa nieruchomości
91.	Zadania wynikające z ustawy Prawo geologiczne i górnicze
92.	Zabytki
93.	Użytkowanie wieczyste
94.	Przekształcenie prawa użytkowania wieczystego w prawo własności
95.	Sprzedaż, nabycie, nieruchomości
96.	Dzierżawa
97.	Decyzje o warunkach zabudowy i zagospodarowania terenu
98.	Decyzje o ustaleniu lokalizacji inwestycji celu publicznego
99.	Podziały nieruchomości
100.	Roszczenia w związku ze zmianą wartości nieruchomości w miejscowym planie zagospodarowania przestrzennego
101.	Zagospodarowanie przestrzenne
102.	Wydawanie wypisów i wyrysów, zaświadczeń i informacji w zakresie planowania i zagospodarowania przestrzennego
103.	Zamówienia publiczne
104.	Baza danych właścicieli nieruchomości dla potrzeb systemu gospodarowania odpadami komunalnymi
105.	Konkursy ekologiczne
106.	Ewidencja umów zawartych na odbieranie odpadów komunalnych

107.	Wnioski o przyłączenie nieruchomości do sieci wodno- kanalizacyjnej
108.	Baza właścicieli nieruchomości posiadających zbiorniki bezodpływowe ścieków i przydomowe oczyszczalnie ścieków na terenie gminy Kowalewo Pomorskie
109.	Zezwolenia na korzystanie z dróg gminnych
110.	Dodatki mieszkaniowe
111.	Gospodarka lokalami mieszkalnymi, socjalnymi i użytkowymi

Załącznik nr 2
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

Kowalewo Pomorskie …….

OŚWIADCZENIE

Oświadczam, że zapoznałem/am się z treścią dokumentów przyjętych Zarządzeniem nr 76/2018 Burmistrza Miasta Kowalewo Pomorskie z dnia 25.05.2018r.
Zobowiązuję się przestrzegać zawartych w nich zapisów oraz informować o każdym naruszeniu zasad ochrony danych osobowych Administratora Danych Osobowych Urzędu Miejskiego w Kowalewie Pomorskim.

……
/podpis/

Załącznik nr 3 cz. 1.
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

Kowalewo Pomorskie, ……

Administrator Danych Osobowych
Urząd Miejski Kowalewo Pomorskie

W N I O S E K

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, proszę o upoważnienie** p. …… pracownika Urzędu Miejskiego w Kowalewie Pomorskim na stanowisku …… do danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku do zbiorów o nazwie:

Lp	Nazwa zbioru danych	Określenie zakresu przetwarzania danych
1.		
2.		
…		

……
/podpis bezpośredniego przełożonego/

Podpis osoby wnioskowanej

……

Załącznik nr 3 cz. 2.
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

Kowalewo Pomorskie, ……

UPOWAŻNIENIE NR ……./…….
DO PRZETWARZANIA DANYCH OSOBOWYCH

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,**

Upoważniam p. …… pracownika Urzędu Miejskiego w Kowalewie Pomorskim na stanowisku …… do danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku ze zbiorów o nazwie:

Lp	Nazwa zbioru danych	Określenie zakresu przetwarzania danych
1		
2		
….		

Traci moc upoważnienie nr ……

Okres trwania upoważnienia od dnia wydania do momentu rozwiązania lub wygaśnięcia stosunku pracy.
Osoba upoważniona do przetwarzania danych objętych zakresem, o których mowa wyżej jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia, oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Administrator Danych Osobowych

……

* niepotrzebne skreślić,

Podpis osoby upoważnionej

……

Załącznik nr 4.
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

Rejestr upoważnień do przetwarzania danych osobowych w Urzędzie Miejskim w Kowalewie Pomorskim

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** jako Administrator Danych Osobowych udziela upoważnienia do przetwarzania danych osobowych osobom:

Nr upoważnienia i data	Osoby upoważnione	Nazwa zbioru danych osobowych	Zmiany i przyczyny wygaśnięcia upoważnienia

Załącznik nr 5 cz. 1.
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

KLAUZULA INFORMACYJNA
dot. Ochrony Danych Osobowych.

Podstawa prawna: Art. 13 ust 1 i 2 Rozporządzenia Parlamentu Europejskiego i rady Europy (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27 kwietnia 2016r. (Dz.Urz.UE nr 119).

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016r. informuję, że:

1. Administratorem Pana/Pani danych osobowych jest BURMISTRZ MIASTA KOWALEWO POMORSKIE, Plac Wolności 1, 87-410 Kowalewo Pomorskie
2. Inspektorem Ochrony Danych Osobowych w Urzędzie Miejskim w Kowalewie Pomorskim jest KAROLINA KOWALSKA. um.kowalewo@wp.pl, 56-684-10-24
3. Pana/Pani dane osobowe przetwarzane są w celu rozpatrzenia wniosku/ realizacji zadań ustawowych samorządu/ na postawie szczegółowych przepisów prawa.
4. Dane osobowe mogą być przekazywane innym organom i podmiotom wyłącznie na podstawie obowiązujących przepisów prawa
5. Pana/Pani dane osobowe będą przechowywane przez okres wynikający z instrukcji kancelaryjnej
6. Posiada Pan/Pani prawo do: dostępu do swoich danych, ich poprawienia, sprostowania, ograniczenia przetwarzania, przenoszenia danych, wniesienia sprzeciwu,
7. Ma Pan/Pani prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych Pana/Panią dotyczących naruszyłoby przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 24 kwietnia 2016r.
8. Podanie danych osobowych jest: obowiązkiem ustawowym/warunkiem realizacji wniosku/warunkiem zawarcia umowy/inne/. Jest Pan/Pani zobowiązany/a do podania danych wymaganych i określonych w formularzu, a konsekwencją niepodania danych będzie nie rozpatrzenie wniosku/nie zawarcie umowy/inne/

Załącznik nr 5 cz. 2.
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

KLAUZULA INFORMACYJNA dla konkretnego wnioskodawcy.

Podstawa prawna: Art. 13 ust 1 i 2 Rozporządzenia Parlamentu Europejskiego i rady Europy (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27 kwietnia 2016r. (Dz.Urz.UE nr 119).

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016r. informuję, że:

1. Administratorem Pana/Pani danych osobowych jest BURMISTRZ MIASTA KOWALEWO POMORSKIE, Plac Wolności 1, 87-410 Kowalewo Pomorskie
2. Inspektorem Ochrony Danych Osobowych w Urzędzie Miejskim w Kowalewie Pomorskim jest KAROLINA KOWALSKA. um.kowalewo@wp.pl, 56-684-10-24
3. Pana/Pani dane osobowe przetwarzane są w celu (np. rekrutacji/rozpatrzenia wniosku) na postawie (*podać podstawę prawną, przepis szczegółowy*)
4. Dane osobowe mogą być przekazywane innym organom i podmiotom wyłącznie na podstawie obowiązujących przepisów prawa
5. Pana/Pani dane osobowe będą przechowywane przez okres wynikający z instrukcji kancelaryjnej
6. Posiada Pan/Pani prawo do: dostępu do swoich danych, ich poprawienia, sprostowania, ograniczenia przetwarzania, przenoszenia danych, wniesienia sprzeciwu,
7. Ma Pan/Pani prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych Pana/Panią dotyczących naruszyłoby przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 24 kwietnia 2016r.
8. Podanie danych osobowych jest: obowiązkiem ustawowym/warunkiem realizacji wniosku/warunkiem zawarcia umowy/inne/*. Jest Pan/Pani zobowiązany/a do podania danych wymaganych i określonych w formularzu, a konsekwencją niepodania danych będzie nie rozpatrzenie wniosku/nie zawarcie umowy/inne/*

*- niewłaściwe skreślić

Załącznik nr 6.
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

Rejestr czynności przetwarzania danych osobowych

Podstawa prawna: Art. 30 Rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016r. w spr. ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w spr. swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE(ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016r. (Dz.Urz. UE nr 119).

Administrator: Urząd Miejski Kowalewo Pomorskie reprezentowany przez Burmistrza Miasta, z siedzibą w Kowalewie Pomorskim, Plac Wolności 1
Inspektor Danych Osobowych: Karolina Kowalska, um.kowalewo@wp.pl, 56 684-1024

Nazwa zbioru oraz referat	Podstawa prawna	Nazwa czynności przetwarzania	Komórka dokonująca czynności	Cel przetwarzania danych	Kategoria osób których dane dotyczą	Kategoria danych osobowych	Zakres przetwarzania danych osobowych	Planowane terminy usunięcia danych	Dane podmiotu przetwarzającego	Kategorie odbiorców którym dane zostały lub zostaną ujawnione	Źródło zbierania danych	Sposób przetwarzania tradycyjny	Ogólny opis tech. i org. środków bezpieczeństwa zastosowanych do ochrony danych
1	2	3	4	5	6	7	8	9	10	11	12	13	14

Załącznik nr 7
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

PROCEDURA SZACOWANIA I ZARZĄDZANIA RYZYKIEM ZWIĄZANYM Z OCHRONĄ DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W KOWALEWIE POMORSKIM

1. WSTĘP

W związku z wejściem w życie RODO Burmistrz Miasta jako ADO podjął szereg działań niezbędnych do zachowania zgodności procedur związanych z przetwarzaniem i ochroną danych osobowych, których jest administratorem jako organ administracji publicznej.
ADO wdrożył odpowiednie środki techniczne i organizacyjne uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych.
Ocenił czy stopień bezpieczeństwa jest odpowiedni, uwzględniając ryzyko wiążące się z przetwarzaniem, a w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawienia lub nieuprawnionego dostępu do danych osobowych przesyłanych , przechowywanych lub w inny sposób przetwarzanych.

1.1 Zasada podejścia opartego na ryzyku

Przeprowadzono szczegółową analizę procesów przetwarzania danych i ocenę ryzyka na jakie przetwarzanie w konkretnym przypadku jest narażone. Takie podejście umożliwia skoncentrowanie się na sytuacjach największego ryzyka, przy jednoczesnym zachowaniu odpowiedniego poziomu ochrony, gdy to ryzyko jest niskie. Administrator jest zobowiązany dostosować środki ochrony przetwarzania danych do skali ryzyka i powinien koncentrować się na zastosowaniu środków redukujących prawdopodobieństwo wystąpienia zagrożeń oraz środki redukujące skutki ich wystąpienia.
Ryzyko należy oszacować na podstawie obiektywnej i rzeczowej analizy, podczas której stwierdza się, czy z operacjami przetwarzania danych osobowych w Urzędzie wiąże się jakieś ryzyko.
Szacowanie ryzyka to proces ciągły, monitorowany i doskonalony. Kluczowym elementem jest przyjęcie określonej systematyki i kolejności działania.

1.2. Założenia i podstawy metody szacowania ryzyka w Urzędzie

Skuteczne zarządzanie ryzykiem wymaga spełnienia następujących warunków:
- zapewnienia powtarzalności i porównywalności wyników
- uwzględnienia stopnia wrażliwości informacji
- uwzględnienia prawdopodobności wystąpienia zdarzenia i jego konsekwencji (skutków)
- uwzględnienia efektu funkcjonowania zabezpieczeń, wpływających na prawdopodobieństwo zajścia zdarzeń, jak i na późniejsze ewentualne konsekwencje ich realizacji

Zastosowano opracowaną do wielkości i charakteru Urzędu metodę szacowania ryzyka spełniająco powyższe założenia. Jej najważniejszymi elementami są: ustalenie kontekstu działalności organizacji oraz identyfikację i klasyfikację zasobów informacyjnych.
Kontekst działalności jest to zestaw czynników zewnętrznych i wewnętrznych, które stanowią o istnieniu Urzędu , jego celach oraz sposobach ich realizacji , oczekiwaniach jakie ma spełnić względem wszystkich interesariuszy. Kontekst działalności jest podstawą do ustalenia kryterium dla oceny ryzyka. Kontekst wraz z dokonaną klasyfikacją zasobów informacyjnych stanowią punkt wyjściowy do identyfikacji ryzyk oraz wynikających z nich zagrożeń.

Kolejnym elementem jest analiza zidentyfikowanych ryzyk, w której oceniamy **prawdopodobieństwo** wystąpienia zagrożenia oraz **skutków** jakie zagrożenie może wywołać. Zidentyfikowane zagrożenia i oceniane ryzyka o określonym stopniu istotności zostają zarejestrowane i udokumentowane na kartach oceny ryzyka i podlegają bieżącej ocenie i monitorowaniu. Na karcie ryzyka dokumentuje się również zasady postepowania z ryzykiem, zadania mające na celu obniżenie ryzyka, kroki jakie należy podjąć w przypadku, gdy ryzyko się zmaterializuje. Przyjmuje się, że ponowna ocen zidentyfikowanego ryzyka nie może być rzadsza niż raz na 12 miesięcy.

2. Określenie kontekstu- informacje i uwarunkowania związane z działalnością Urzędu

Na ryzyko w zakresie ochrony danych wpływają czynniki zarówno wewnętrzne jak i zewnętrzne. Działalność Urzędu wiąże się ze spełnieniem oczekiwań wielu stron. Strony te i ich oczekiwania stanowią kontekst działalności Urzędu, a oczekiwania względem przepływu i bezpieczeństwa informacji są kryteriami ryzyka, które powinny podlegać bieżącej analizie i ocenie. Elementy stanowiące zewnętrzny i wewnętrzny kontekst organizacyjny zostały zidentyfikowane i opisane w tabeli poniżej.

2.1.Kontekst zewnętrzny

LP	Podmiot	Wpływ Urzędu na aspekt TAK/NIE	Cel/wymagania/ oczekiwania względem Urzędu
1.	Mieszkańcy	NIE	Oczekiwanie sprawnego działania Urzędu, racjonalne kosztowo realizowanie zadań administracji publicznej
2.	Starostwo Powiatowe, Urząd Marszałkowski, Wojewódzki	NIE	Sprawna realizacja zadań administracyjnych (zleconych) powierzonych urzędowi, podejmowanie działań w ramach ustalonego prawa, stanowienie racjonalnego prawa lokalnego
3.	Instytucje publiczne: Biuro Wyborcze, GUS, pozostali	NIE	Sprawna realizacja zadań powierzonych
4.	Jednostki organizacyjne własne: placówki oświatowe, MGOK, MGOPS, ZGKiM	TAK	Utrzymanie wsparcia dla własnych jednostek organizacyjnych, w tym w zakresie dostarczania usług elektronicznych (łącze internetowe, sprawna komunikacja z urzędem)
5.	Organizacje pozarządowe na terenie gminy: OSP, LKS, OPP	TAK częściowo	Wsparcie dla działalności klubów, patronat nad wydarzeniami

2.2. Kontekst wewnętrzny

LP	Opis	Wpływ Urzędu na aspekt TAK/NIE	Cel/wymagania/ oczekiwania względem Urzędu
1.	Rada Miejska w Kowalewie Pom.	TAK częściowo	Realizacja zadań Urzędu wynikających ze statutu oraz uchwał rady, nadzorowanie pracy burmistrza oraz podległych gminie jednostek organizacyjnych
2.	Burmistrz i kadra kierownicza Urzędu	TAK	Bezpieczeństwo zasobów informacyjnych, dostęp do bieżącej informacji zarządczej, unikanie i zapobieganie incydentom związanym z utratą bądź zniszczeniem danych
3.	Pracownicy Urzędu	TAK	Bezpieczeństwo pracy użytkowników, dostępność środków wymiany informacji, uzyskanie informacji na poziomie umożliwiającym sprawne realizowanie powierzonych zadań, zabezpieczenie danych osobowych na stanowisku pracy.
4.	Systemy wsparcia informacji	TAK	Systemy wymiany informacji działają w oparciu o sprawną infrastrukturę sieciowo-serwerową. Wymagają utrzymania jej na poziomie pozwalającym na sprawne przekazywanie danych między aplikacjami i bazami danych a terminalami. Utrzymanie sprawności funkcjonowania wymaga adekwatnych nakładów finansowych.
5.	Infrastruktura informatyczna (sieci, węzły komunikacyjne, serwery)	TAK	Infrastruktura informatyczna pozwala na sprawne przekazywanie danych pomiędzy aplikacjami, bazami danych. Utrzymanie sprawności funkcjonowania wymaga adekwatnych nakładów finansowych
6.	Obsługa informatyczna	TAK	Urząd ma własnego informatyka- 1 etat
7.	e-urząd	TAK	Usługa wymaga wsparcia technicznego służb informatycznych urzędu, utrzymania odpowiedniej dostępności systemu, utrzymania mechanizmów autoryzacji przesyłanych danych pomiędzy klientem a Urzędem.

3. Opis przetwarzanych danych i ich klasyfikacja

3.1. Aktywa Urzędu, które wiążą się z przetwarzaniem danych osobowych

Posiadane zasoby opisane zostały szczegółowo w załączniku nr 6- Rejestr czynności przetwarzania danych osobowych do Polityki Bezpieczeństwa Danych Osobowych.
Polityka określa również odpowiedzialność pracowników za prawidłowe przetwarzanie danych osobowych.

3.2. Klasyfikacja posiadanych aktywów informacyjnych

Zidentyfikowane zasoby opisane są w „Karcie klasyfikacji zasobów i aktywów informacyjnych" stanowiących **załącznik 6.1** do Procedury. W karcie klasyfikacyjnej uwzględniono kto jest właścicielem danego zasobu informacyjnego, czyli odpowiedzialnym za jego przetwarzanie oraz jakie wymagania bezpieczeństwa zidentyfikowano dotychczas w celu

jego zabezpieczenia. Zidentyfikowane zasoby informacyjne poddane zostały analizie pod względem ich istotności w Urzędzie. Określenie ich wartości dla działalności Urzędu następuje poprzez przydzielenie im odpowiednich ocen w obszarach poufności (P), dostępności (D) i integralności (I) w skali 1-3 na każdym poziomie. W celu uporządkowania klasyfikacji, zasoby które mają podobną wartość oraz podobne wymogi bezpieczeństwa można łączyć w grupy.

3.2.1. Poziom poufności (P)

Poziom	Rodzaj informacji
1	Informacje ogólnodostępne- informacja publiczna
2	Dane chronione RODO za wyjątkiem danych wrażliwych, informacje które przetwarzane są w wielu instytucjach (np. firmy telekomunikacyjne, dostawcy mediów), również chronione informacje wewnętrzne organizacji, których ujawnienie nie wiąże się z sankcjami karnymi lub odszkodowawczymi, jednak może wiązać się z niewielkimi stratami, także wizerunkowymi Urzędu
3	Informacje chronione przede wszystkim art. 9. Ust 1 RODO (dane wrażliwe), również informacje objęte tajemnicą wynikającą z innych aktów prawnych (np. ordynacja podatkowa, tajemnica bankowa, tajemnica przedsiębiorstwa i pozostałych). Informacja, których ujawnienie może wiązać się z sankcjami karnymi lub odszkodowawczymi oraz mogą zagrozić istnieniu podmiotu (tajemnica przedsiębiorstwa)

3.2.2. Poziom dostępności (D)

Poziom	Rodzaj informacji
1	Informacje, które są konieczne do realizacji zdania, a przerwa w ich dostępie nie może być dłuższa niż 5-7 dni roboczych
2	Informacje, które są konieczne do realizacji zdania, a przerwa w ich dostępie nie może być dłuższa niż 3-5 dni roboczych
3	Informacje muszą być dostępne w sposób nieprzerwalny, brak dostępu może w skrajnych okolicznościach skutkować sankcjami karnymi lub odszkodowawczymi

3.2.3. Poziom integralności (I)

Poziom	Rodzaj informacji
1	Naruszenie integralności informacji jest łatwe do wykrycia i naprawienia, skutki wywołane nieprawidłową informacją są łatwe do przewidzenia i naprawienia
2	Naruszenie integralności informacji jest możliwe do wykrycia i naprawienia, skutki wywołane wadliwą informacją są możliwe do skorygowania , wymaga to jednak pewnego nakładu pracy i/lub wiąże się z poniesieniem niewielkich nakładów finansowych
3	Naruszenie integracji informacji jest trudne lub wręcz nie możliwe do naprawienia, skutki wywołane wadliwą informacją wiążą się z poważnymi sankcjami (np. odszkodowawczymi lub karnymi), usunięcie bądź skorygowanie skutków wiąże się z poniesieniem znaczących nakładów finansowych.

3.2.4. Poziom ochrony danych osobowych

Na podstawie poziomu poufności, dostępności i integralności aktywu (danych) określa się poziom ochrony. Poziom ochrony wynika z najwyższej, przyznanej oceny dla danych. Przyjęta skala obejmuje I, II i III poziom ochrony. W razie potrzeby można stosować oznaczenia poziomów bezpieczeństwa na nośnikach informacji (teczki, segregatory, dyski).

4. Szacowanie ryzyka.

4.1.Identyfikacja zagrożenia

Dla każdej grupy aktywów (zbioru danych osobowych) określa się podatność i zagrożenia z nich wynikające. W analizie bierzemy pod uwagę trzy grupy zagrożeń związanego z przetwarzaniem informacji.

Zagrożenie dla poufności- zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.

Zagrożenie dla dostępności- zapewnienie, że dane są dostępne i możliwe do wykorzystania na żądanie, w założonym czasie przez osobę autoryzowana (z upoważnieniem).

Zagrożenie dla integralności – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

4.2.Identyfikacja podatności na zagrożenia.

Identyfikacja podatności na zagrożenia związane z dokumentacją, teleinformatyką, sprzętem, otoczeniem fizycznym i infrastrukturą oraz z działaniami pracowników została przedstawiona w tabeli stanowiącej załącznik nr 6.2 do Procedury Szacowania i Zarządzania Ryzykiem

4.3.Szacowanie poziomu ryzyka

Każde z ocenianych zagrożeń dla aktywów (danych) jest oceniane pod kątem prawdopodobieństwa wystąpienia. Przyjęto pięciostopniową skalę oceny **i** przypisano jej poszczególne wartości.

4.3.1. Metodologia.

Prawdopodobieństwo	Poziom	Opis
Prawie pewne	5	Zdarzenie występuje min. raz w miesiącu
Prawdopodobne	4	Zdarzenie występuje min. raz na kwartał
Możliwe	3	Zdarzenie występuje min. raz w roku
Mało prawdopodobne	2	Zdarzenie występuje min. raz na trzy lata
Rzadkie	1	Zdarzenie NIE występuje, a prawdopodobieństwo wystąpienia jest znikome

Każde zagrożenie oceniane jest pod kątem wartości skutków i poziomu zagrożeń.

Stopień	Poziom	Skutki finansowe	Odpowiedzialność	Reputacja
Bardzo wysoki	5	Powyżej 100tys.zł	Złamanie przepisów prawa, odpowiedzialność karna (ograniczenie, pozbawienie wolności) lub cywilna	Negatywne opinie medialne w skali kraju
Wysoki	4	10tys.zł-100tys.zł	Złamanie przepisów prawa, odpowiedzialność finansowa lub służbowa.	Negatywne opinie medialne częściowo w mediach krajowych, regionalnych oraz lokalnych
Średni	3	1tys.zł-10tys.zł	Złamanie przepisów prawa, odpowiedzialność służbowa,	Negatywne opinie w mediach lokalnych,
Niski	2	100zł- 1000zł	Naruszenie procedur, brak bezpośredniej odpowiedzialności	Negatywne opinie bez udziału mediów,
Bardzo niski	1	Brak skutków	Nie ma naruszenia przepisów, znikome naruszenie procedur,	Brak wpływu na reputację,

Po określeniu prawdopodobieństwa wystąpienia poszczególnych incydentów oraz po przeprowadzeniu szacowania następstw określa się poziom ryzyka jako iloczyn prawdopodobieństwa i skutków.

		SKUTEK				
		Bardzo niski	**Niski**	**Średni**	**Wysoki**	**Bardzo wysoki**
PRAWDOPODOBIEŃSTWO	**Poziom**	**1**	**2**	**3**	**4**	**5**
Prawie pewne	5	5- Ś	10- W	15- K	20- K	25- K
Prawdopodobne	4	4- Ś	8- W	12- K	16- K	20 – K
Możliwe	3	3- Ś	6 - Ś	9- W	12- W	15 – K
Mało prawdopodobne	2	2- N	4 – Ś	6- Ś	8- W	10 – W
Rzadkie	1	1- N	2 - N	3 - Ś	4- Ś	5- Ś

Tabela opisująca konieczność podjęcia określonych działań w zależności od zdefiniowanego poziomu ryzyka dla poszczególnych zagrożeń.

Poziom ryzyka	Zakres punktowy	Opis działania
NISKI (N)	1-2	Poziom ryzyka akceptowalny. Działania podejmowane w zależności od wymaganych nakładów
ŚREDNI (S)	3-6	Poziom ryzyka akceptowalny. Działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania.
WYSOKI (W)	7-10	Poziom ryzyka nieakceptowalny. Działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania.
KRYTYCZNY (K)	11-25	Poziom ryzyka nietolerowany. Wymaga natychmiastowego działania.

4.3.2. Karta ryzyka.

Dla zidentyfikowanego ryzyka o poziomie Średni (Ś), Wysoki (W) i Krytyczny (K) zakłada się kartę ryzyka, w której określa się:
- zidentyfikowane zagrożenie,
- podatność, czyli możliwość przyczyny wystąpienia zidentyfikowanego zagrożenia, które mogą doprowadzić do jego realizacji i powstania straty,
- przyjęty poziom prawdopodobieństwa wystąpienia zagrożenia,
- przyjęty poziom skutku potencjalnego wystąpienia zagrożenia,
- oszacowany poziom ryzyka (niski, średni, wysoki, krytyczny)
- podjęte działania w związku ze zidentyfikowanym ryzykiem,
- monitoring ryzyka,

Kartę ryzyka Użytkownik Zbioru przedkłada ADO po 12 miesiącach analizy. Pozwala to na ocenę podjętych działań i oceny poziomu wystąpienia zagrożenia. ADO ocenia, czy można zmniejszyć poziom ryzyka dla danego zbioru.
Wzór karty ryzyka stanowi załącznik nr 6.2 do Procedury Szacowania i Zarządzania Ryzykiem

4.3.3. Zestawienie zidentyfikowanych zagrożeń i ryzyk wraz z określeniem ich oszacowanego poziomu

Zestawienie sporządza ADO po dokonaniu przez Użytkowników Zbioru analiz ryzyka. Po minimum 12 miesiącach ADO dokonuje ponownej oceny występujących w Urzędzie Miejski w Kowalewie Pomorskim zagrożeń. Po sprawdzeniu Kart ryzyka pod kątem oceny skuteczności prowadzonych działań i zastosowanych rozwiązań ADO może zmniejszyć poziom ryzyka.

Załącznik nr 6.1 do PROCEDURY SZACOWANIA
I ZARZĄDZANIA RYZYKIEM

„Karta klasyfikacji zidentyfikowanych zasobów i aktywów informacyjnych”

Administrator: Burmistrz Miasta Kowalewo Pomorskie
Inspektor Ochrony Danych Osobowych: Karolina Kowalska, um.kowalewo@wp.pl, 56 684-1024

Nazwa zbioru	Komórka dokonująca czynności	Poziom poufności (P)	Poziom Dostępności (D)	Poziom integralności (I)	Poziom zbioru

Załącznik nr 6.2 do PROCEDURY SZACOWANIA
I ZARZĄDZANIA RYZYKIEM

Identyfikacja podatności na zagrożenia.

Zagrożenie	Podatność	Prawdopodobieństwo (1)	Skutek (2)	Poziom ryzyka (1)x(2)
PERSONEL				
Np. Nieprzestrzeganie zasady „czystego biurka”	Np. Bałaganiarstwo, pospiech, Nieznajomość zasad ochrony danych osobowych obowiązujących w jednostce			
Np. pozostawienie klienta w miejscu przetwarzania danych (biuro) bez nadzoru	Np. brak świadomości, że tego typu działania mogą stworzyć możliwość dostępu osób nieuprawnionych do danych. Nieznajomość zasad ochrony danych osobowych obowiązujących w jednostce			
Np. pozostawienie kluczy od pomieszczeń, szaf w drzwiach	Np. brak znajomości procedury kluczowej,			
Np. zagubienie dokumentów, kluczy, pieczątek, płyt CD	Np. Nieprzestrzeganie zakazu wynoszenia dokumentów na zewnątrz. Nieznajomość zasad ochrony danych osobowych obowiązujących w jednostce			
Np. pozostawienie pendriwa w niepowołanym nośniku	Np. Bałaganiarstwo, pospiech, Nieznajomość zasad ochrony danych osobowych obowiązujących w jednostce			
Np. podszycie się osoby nieuprawnionej pod wnioskodawcę				
inne				
SPRZĘT				
Np. Uszkodzenie podczas obsługi	Niewłaściwa obsługa urządzenia przez pracownika, błędna instalacja, brak przeszkolenia pracownika w zakresie obsługi			
Np. Uszkodzenie przez czynniki zewnętrzne- kurz, wilgoć,				

Np. komputer starszy niż 5-6 lat	Zawodność sprzętu komputerowego po określonym czasie			
inne				
INFRASTRUKTURA				
Np. Włamanie i kradzież.	Niewłaściwe zabezpieczenie okien, drzwi,			
Np. pęknięcie rury	Brak przeglądów, stara, wadliwa sieć wodno-kanalizacyjna,			
Np. pożar,	Brak czujek dymowych, sprzęt gastronomiczny (czajniki) w biurach			
Np. Kurz, wilgoć	Niewłaściwa dbałość personelu gospodarczego			
Np.. skoki zasilania	Wadliwa Instalacja elektryczna, brak przeglądów			
Np. celowe uszkodzenie, sabotaż				
inne				
TELEINFORMATYKA				
Atak hakerski	Niewystarczające zabezpieczenie systemu			
Wykorzystanie sprzętu przez nieautoryzowanego użytkownika	Niewłaściwe ustawienie monitora w biurze, Udostępnienie hasła osobom nieupoważnionym			
Przekazanie do serwisu (naprawy) dysków z danymi osobowymi				
Wirusy i inne szkodliwe oprogramowania	Sprawdzanie oprogramowania, zamontowanie oprogramowania z niepewnego źródła,			
Kradzież serwera	Okna bez zabezpieczeń			
Dostęp nieautoryzowany	Przekazanie haseł, słabe zabezpieczenia			
inne				

Załącznik nr 6.3 do
PROCEDURY SZACOWANIA I ZARZĄDZANIA RYZYKIEM

Karta Ryzyka nr ……

Rejestr czynności	Komórka przetwarzająca	Zagrożenie	Podatność*	Prawdopodobieństwo	Skutek	Poziom ryzyka

* Podatność, dzięki której może dojść do zagrożenia, a w jego wyniku powstania straty. Jest to luka, uchybienie, słaby punkt, którego istnienie powoduje, że słaby zagrożenie jest mniej lub bardziej podatne.

1. Postępowanie ze zidentyfikowanym ryzykiem i podjęte działania, które ma na celu zminimalizowanie ryzyka poprzez wyeliminowanie podatności

2. Informacja o ryzyku i skuteczności prowadzonych działań, czyli monitorowanie ryzyka.

Sporządzający:……..

Załącznik nr 8
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

Zgłoszenie w sprawie naruszenia ochrony danych osobowych

Podstawa prawna: Art. 30 ust. 5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27 kwietnia 2016r. (Dz.Urz.UE nr 119).

Administrator: Burmistrz Miasta Kowalewo Pomorskie, Plac Wolności 1, 87-410 Kowalewo Pomorskie. 56 684-1024
Inspektor Ochrony Danych Osobowych: Karolina Kowalska, Urząd Miejski, Plac Wolności 1, 87-410 Kowalewo Pomorskie, 56 684-1024

Zgłoszenie dotyczy danych ze zbioru:……..
Zgłaszający: ……
Data zgłoszenia: …….

1.	Charakter naruszenia:	
2.	Kategoria i liczba osób, których dane dotyczą	
3.	Możliwe skutki naruszenia	
4.	Podjęte działania w celu zminimalizowania możliwych skutków naruszenia	
5.	Data wpisania do rejestru naruszeń i nr w rejestrze (art. 33 ust. 5 RODO)	

Załącznik nr 9
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Kowalewie Pomorskim

Rejestr naruszeń ochrony danych osobowych

Podstawa prawna: Art. 30 ust. 5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27 kwietnia 2016r. (Dz.Urz.UE nr 119).

Administrator: Burmistrz Miasta Kowalewo Pomorskie, Plac Wolności 1, 87-410 Kowalewo Pomorskie. 56 684-1024
Inspektor Ochrony Danych Osobowych: Karolina Kowalska, Urząd Miejski, Plac Wolności 1, 87-410 Kowalewo Pomorskie, 56 684-1024

Lp.	Data naruszenia	Rodzaj naruszenia	Opis okoliczności	Możliwe skutki naruszenia	Podjęte działania w celu zminimalizowania możliwych skutków naruszenia	Zgłoszenie do prezesa Urzędu ochrony Danych Osobowych (tak/nie)- data, nr zgłoszenia, nr sprawy