Or.120.40.2018

Zarządzenie Nr 40/2018
Burmistrza Zabłudowa
z dnia 12 czerwca 2018 r.
w sprawie wprowadzenia „Polityki Ochrony Danych Osobowych”
w Urzędzie Miejskim w Zabłudowie.

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (tj. Dz. U. z 2018r., poz. 994) oraz art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE, L 119 z 4.05.2016 t.)

Zarządza się, co następuje:

§ 1.

Wprowadza się w Urzędzie Miejskim w Zabłudowie „Politykę ochrony danych”, stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Wykonanie Zarządzenia powierza się Inspektorowi Ochrony Danych.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do Zarządzenia nr 40/2018
Burmistrza Zabłudowa
z dnia 12 czerwca 2018 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

w Urzędzie Miejskim w Zabłudowie

Zabłudów, 12 czerwca 2018 r.

Spis treści

1 Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

1.1 Administrator Danych osobowych.

Administratorem Danych jest Burmistrz Zabłudowa z siedzibą w Zabłudowie 16-060 ul. Rynek 8.

1.2 Inspektor Ochrony Danych.

Wyznacza się Inspektora Ochrony Danych

Dane teleadresowe: Inspektor Ochrony Danych, ul. Rynek 8, 16-060 Zabłudów.

Adres e-mail: iod@zabludow.pl

1.3 Obszar przetwarzania danych.

Obszarem przetwarzania danych jest budynek Urzędu Miejskiego w Zabłudowie ul. Rynek 8.

1.3.1 Definicje.

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi, Podmiotowi przetwarzającemu i pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Administrator Systemu Informatycznego (ASI) - informatyk lub osoba wyznaczona przez firmę informatyczną odpowiedzialna za prawidłowe działanie i bezpieczeństwo infrastruktury IT.

RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r.

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie,

przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (legendy), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Anonimizacja- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

2 Analiza ryzyka.

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli Administrator nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

Ocena skutków musi być wykonana z udziałem Inspektora Ochrony Danych.

2.1 Opis operacji przetwarzania.

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku ***nr 1 – Rejestr czynności przetwarzania.***
2. Opis zbiorów powinien obejmować takie informacje, jak:
   a. nazwę zbioru
   b. opis celów przetwarzania
   c. charakter, zakres danych osobowych
   d. odbiorcy danych
   e. funkcjonalny opis operacji przetwarzania
   f. aktywa służące do przetwarzania danych osobowych
   g. informacja o konieczności przeprowadzenia oceny skutków dla zbioru

2.2 Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO).

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia obowiązków prawnych wobec danych w zbiorach.

W szczególności należy zapewnić, że :

1. dane te są legalnie przetwarzane
2. dane te są adekwatne w stosunku do celów przetwarzania
3. dane te są przetwarzane przez określony czas
4. wobec tych osób wykonano tzw. obowiązek informacyjny wraz ze wskazaniem ich praw
5. opracowano klauzule informacyjne dla powyższych osób załącznik ***nr 2 – Klauzule informacyjne***
6. istnieją umowy powierzenia z podmiotami przetwarzającymi zgodnie z załącznikiem ***nr 3 – wzór umowy powierzenia danych*** umowy te są rejestrowane wg załącznika

nr 4 – rejestr umów powierzenia danych, rejestr ten prowadzi Inspektor Ochrony Danych.

7. potwierdzenie spełnienia powyższych wymagań prawnych RODO rejestruje się w rejestrze czynności przetwarzania, który opisany jest załącznikiem ***nr 1 – Rejestr czynności przetwarzania***, rejestr prowadzi Inspektor Ochrony Danych.

2.3 Analiza ryzyka.

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów lub dla procesów przetwarzania.

2.3.1 Definicje.

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.

2. Incydent - naruszenie ochrony danych osobowych, prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

3. Zagrożenie - potencjalne naruszenie (potencjalny incydent).
4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

2.3.2 Wyznaczenie zagrożeń.

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania.

2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.

2.3.3 Wyliczenie ryzyka dla zagrożeń.

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania.
2. Skalę prawdopodobieństwa prezentuje Tabela A.
3. Administrator określa Skutki (**S**) wystąpienia incydentów, uwzględniając straty finansowe, utratę reputacji, sankcje, skutki karne
4. Proponowaną Skalę skutków prezentuje Tabela B
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków na podstawie wzoru: **P * S = R**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA**
Niskie w 100 próbach podejmuje do 20 szans na wystąpienie	1
Średnie w 100 próbach podejmuje od 21 do 79 szans na wystąpienie	2
Wysokie w 100 próbach podejmuje ponad 80 szans na wystąpienie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA**
Małe - straty materialne do wysokości jednej pensji średniej krajowej - w opinii publicznej poruszane w lokalnych mediach	1
Średnie - straty materialne od jednej do trzech pensji średnich krajowych - w opinii publicznej poruszane w mediach ogólnokrajowych	2
Duże - straty materialne powyżej wysokości trzech średnich krajowych pensji - przestępstwo	3

2.3.4 Porównanie wyznaczonego ryzyka ze skalą i określenie dalszego postępowania z ryzykiem.

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
2. Skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
ryzyko akceptowalne	1-2
ryzyko opcjonalne	3-6
ryzyko nieakceptowalne	9

2.3.5 Postępowanie z ryzykiem.

Po określeniu poziomu ryzyka podejmuje się stosowne działania. Analizę dokonuje się na podstawie załącznika ***nr 5 – Analiza ryzyka.*** Administrator podejmuje decyzję o zastosowaniu działań odnośnie wykazanego ryzyka.

Administrator może:

1. Zaakceptować ryzyko – poziom zabezpieczeń jest odpowiedni, należy monitorować zmiany poziomu ryzyka.
2. Zdecydować o obniżeniu poziomu ryzyka poprzez zastosowanie działań:
    a. Przeniesienie ryzyka na inny podmiot.
    b. Unikanie ryzyka poprzez eliminowanie działań powodujących ryzyko.
    c. Redukcja ryzyka poprzez zastosowanie odpowiednich działań.

2.3.6 Ponowna analiza ryzyka.

Ponowna analiza ryzyka przeprowadzana jest co najmniej raz w roku cyklicznie lub po wystąpieniu zmian takich jak przetwarzanie nowych zbiorów, działania w nowych procesach przetwarzania danych lub w przypadku zmiany prawa.

2.4 Plan postępowania z ryzykiem.

1. Jeśli Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

3 Upoważnienia.

1. Administrator odpowiada za nadawanie i odbieranie upoważnień do przetwarzania danych w zbiorach w postaci papierowej oraz w systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisów obowiązującego prawa.
3. Upoważnienia nadawane są na wniosek kadry kierowniczej. Upoważnienia określają zakres operacji na danych tj. wgląd, tworzenie, usuwanie, przekazywanie. Upoważnienia nadawane są w formie udokumentowanego zakresu obowiązków.
4. Wzór upoważnienia reguluje załącznik ***nr 6 – Upoważnienie do przetwarzania danych.***
5. Upoważnienie oraz jego anulowanie realizowane jest w oparciu o wniosek, którego wzór realizuje załącznik nr ***7 – Wniosek o nadanie upoważnienia do przetwarzania danych osobowych.***
6. Wniosek
7. Inspektor Ochrony Danych może prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych w formie pisemnej, elektronicznej lub łączonej.

4 Środki organizacyjne i techniczne zabezpieczające dane osobowe.

Administrator jest zobowiązany do stosowania zabezpieczeń techniczno-organizacyjnych adekwatnych do zagrożeń naruszenia praw i wolności osób.

1. Administrator opracowuje procedury stosowania zabezpieczeń techniczno-organizacyjnych. Wykaz tych procedur opisuje załącznik ***nr 8 – procedury techniczno-organizacyjne.***
2. Administrator prowadzi uproszczony wykaz stosowanych zabezpieczeń w postaci ***załącznika nr 9 – Zabezpieczenia techniczno-organizacyjne.***
3. Jeśli zajdzie taka potrzeba, po przeprowadzeniu analizy ryzyka, instrukcja i wykaz powinny być aktualizowane.

5 Regulamin Ochrony Danych Osobowych.

Regulamin Ochrony Danych Osobowych reguluje kwestie związane z bezpieczeństwem przetwarzania danych osobowych. Regulamin jest dokumentem niepublicznym, gdyż zawiera wskazówki dotyczące zabezpieczeń. Regulamin powinien być aktualizowany a z jego zmianami powinni zapoznać się wszyscy uprawnieni pracownicy.

Po zapoznaniu się z treścią regulaminu, osoby przetwarzające dane w instytucji zobowiązane są do potwierdzenia zapoznania się z regulaminem i deklaracji jego przestrzegania. Wzór deklaracji reguluje ***nr 10 – Oświadczenie o poufności.***

6 Szkolenia.

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu lub zapoznana z przepisami o ochronie danych osobowych.
2. Za przeprowadzenie szkolenia odpowiada Inspektor Ochrony Danych Osobowych.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą załącznika ***nr 11 – Program Szkolenia.***
4. Uczestnicy szkolenia zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania na podstawie załącznika ***nr 10 – Oświadczenie o poufności.***
5. Wzór zaświadczenia stwierdzającego odbycie szkolenia reguluje załącznik ***nr 12 – Zaświadczenie o odbyciu szkolenia.***

7 Instrukcja postępowania z incydentami.

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub Inspektora Ochrony Danych
2. Do typowych podatności 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 (niestosowanie się do regulaminu przetwarzania danych osobowych)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu lub pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom

nieupoważnionym, świadome zniszczenie dokumentów lub danych, działanie wirusów i innego szkodliwego oprogramowania)

4. W przypadku stwierdzenia wystąpienia incydentu, Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – ***Załącznik nr 13 – Rejestracja Incydentu.***
6. Zgłoszenia incydentu do Inspektora Danych Osobowych dokonuje pracownik za pomocą załącznika ***14 – zgłoszenie incydentu.***
7. W przypadku wystąpienia znacznego naruszenia ochrony danych osobowych i konieczności zgłoszenia incydentu do organu nadzorczego wykonuje się protokół wg wzoru ***15- Protokół naruszenia danych osobowych.***
8. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
9. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – Inspektor Ochrony Danych zgłasza je organowi nadzorczemu.
10. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Inspektor Ochrony Danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

8 Audyty

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W tym celu Administrator stosuje procedurę audytów ***Załącznik nr 16 – Sprawdzenia i Audyty.***

9 Procedura przywrócenia dostępności danych osobowych

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

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

LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych	Nazwa współadministratora i dane kontaktowe	Nazwa podmiotu przetwarzającego i dane kontaktowe	Kategorie odbiorców	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
															Transfer do kraju trzeciego lub organizacji międzynarodowej	Zabezpieczenia
1.																
n.																

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

Klauzula – tę treść kandydaci umieszczają na CV.
Na podstawie art.6 ust.1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb aktualnej i przyszłych rekrutacji.

Informacja – informacja zawarta w ofercie o pracę.
Na podstawie art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, że:
1) administratorem Pana/i danych osobowych jest Burmistrz Zabłudowa z siedzibą w Zabłudowie przy ulicy Rynek 8.
2) z Inspektorem Ochrony Danych można się skontaktować drogą mailową – iod@zabludow.pl
3) Pana/i dane osobowe przetwarzane będą dla potrzeb aktualnej i przyszłych rekrutacji - na podstawie Art. 6 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. oraz Kodeksu Pracy z dnia 26 czerwca 1974 r.
4) Pana/i dane osobowe przechowywane będą przez okres 2 lat od złożenia dokumentów.
4) odbiorcami Pana/i danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie osobnych przepisów.
5) posiada Pan/i prawo do żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie.
6) ma Pan/i prawo wniesienia skargi do organu nadzorczego.
7) podanie danych osobowych jest obligatoryjne w oparciu o przepisy prawa a w pozostałym zakresie jest dobrowolne.
8) Pani/Pana dane będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania, konsekwencją takiego przetwarzania będzie kontakt tylko z wybranymi kandydatami
9) Więcej informacji dostępnych na stronie: http://bip.um.zabludow.wrotapodlasia.pl/dane-osobowe.html

Informacja dla pracowników:
Na podstawie art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) zwanym dalej RODO informuję, że:
1) administratorem Pana/i danych osobowych jest Burmistrz Zabłudowa z siedzibą w Zabłudowie przy ulicy Rynek 8,
2) z Inspektorem Ochrony Danych można się skontaktować drogą mailową – iod@zabludow.pl
3) celem przetwarzania jest zatrudnianie, pomoc socjalna, zapewnienie komercyjnych świadczeń socjalnych oraz bezpieczeństwo i organizacja pracy
- na podstawie Art. 6 ust. 1 lit. c RODO oraz Kodeksu Pracy z dnia 26 czerwca 1974 r. oraz
- na podstawie Art. 6 ust. 1 lit. f, jako niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (monitoring wizyjny, monitoring systemów informatycznych, wewnętrzna identyfikacja wizualna pracowników)
4) odbiorcami Pana/i danych osobowych będą
• Medycyna pracy

- Komercyjna opieka medyczna
- Pakiet socjalny (np. programy emerytalne, ubezpieczenia grupowe, karty sportowe dla pracowników)
- Biura podróży (na potrzeby podróży służbowych)

5) Pana/i dane osobowe przechowywane będą przez okres 50 lat, na podstawie Kodeksu Pracy a w pozostałych przypadkach do ustania przyczyn biznesowych oraz do momentu odwołania zgody.
6) posiada Pan/i prawo do żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie
7) ma Pan/i prawo wniesienia skargi do organu nadzorczego.
8) podanie danych osobowych jest obligatoryjne w oparciu o przepisy prawa a w pozostałym zakresie jest dobrowolne.

Informacja dla kontrahentów i osób zatrudnionych na umowę zlecenie, dzieło etc.
Na podstawie art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) zwanym dalej RODO informuję, iż:
1) administratorem Pani/Pana danych osobowych jest Burmistrz Zabłudowa z siedzibą w Zabłudowie przy ulicy Rynek 8
2) z Inspektorem Ochrony Danych można się skontaktować drogą mailową - iod@zabludow.pl
3) Pana/i dane osobowe przetwarzane będą w celu realizacji umowy - na podstawie Art. 6 ust. 1 lit. b RODO
4) odbiorcami Pana/i danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych lub Podmioty uczestniczące w realizacji zlecenia.
5) Pana/i dane osobowe przechowywane będą przez okres 6 lat / lub w oparciu o uzasadniony interes realizowany przez administratora,
6) posiada Pan/i prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania.
7) ma Pan/i prawo wniesienia skargi do organu nadzorczego
8) podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych może skutkować odmową zawarcia umowy.

Klauzula informacyjna dla usług oferowanych na podstawie umowy.
Na podstawie art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. zwanym dalej RODO informuję, że:

1) administratorem Pana/i danych osobowych jest Burmistrz Zabłudowa z siedzibą w Zabłudowie ul. Rynek 8, 16-060.
2) kontakt z Inspektorem Ochrony Danych możliwy jest mailowo: iod@zabludow.pl
3) Pana/i dane osobowe przetwarzane będą w celu zapewnienia realizacji umowy.
4) Podstawą przetwarzania danych jest uzasadniony interes administratora jakim jest konieczność rozliczania kosztów oraz świadczenia usługi.
5) Odbiorcami Pana/i danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych lub podmioty uczestniczące w realizacji zlecenia.
6) Pana/Pani dane osobowe przechowywane będą przez okres określony obowiązującymi przepisami prawa.
7) posiada Pan/i prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie.

8) ma Pan/i prawo wniesienia skargi do organu nadzorczego
9) podanie danych osobowych jest warunkiem zawarcia umowy jednakże niepodanie danych w zakresie wymaganym przez administratora może skutkować nie zawarciem umowy.
10) Pana/i dane nie będą poddane zautomatyzowanym podejmowaniu decyzji (profilowaniu).
11) Pani/Pana dane nie będą przekazane odbiorcy w państwie trzecim lub organizacji międzynarodowej.

Ochrona Danych Osobowych – Obowiązek Informacyjny.

Informacja.

Informujemy, że podmiotem przetwarzającym Państwa dane osobowe, a więc Administratorem Danych Osobowych (ADO) jest Burmistrz Zabłudowa z siedzibą w Zabłudowie przy ulicy Rynek 8 nazywany dalej „urząd".

W sprawach ochrony danych osobowych został powołany Inspektor Ochrony Danych (IOD), do którego można kontaktować się za pośrednictwem:

e-mail: iod@zabludow.pl
telefonicznie: Pocztowo: Inspektor Ochrony Danych, Urząd Miejski w Zabłudowie, ul. Rynek 8, 16-060 Zabłudów
Przez platformę ePUAP:
Przez Cyfrowy Urząd:
Gdy mowa o *danych osobowych* należy przez to rozumieć dane mogące w sposób bezpośredni lub pośredni ale jednoznaczny, bez nadmiernych kosztów, czasu i działań, określić konkretną osobę fizyczną. Danymi osobowymi nie są dane firm.

Czyje dane osobowe są przetwarzane.

Urząd przetwarza dane osobowe osób zamieszkujących i zameldowanych na terenie gminy Zabłudów, pracowników i kandydatów do pracy w urzędzie oraz osób zainteresowanych - składających pisma do urzędu i załatwiających sprawy w tutejszym urzędzie np. akty zgonu, akty zawarcia związku małżeńskiego, dostęp do informacji publicznej etc.

Źródło danych osobowych.
W przypadku:

1. Realizacji celu publicznego na podstawie odrębnych przepisów lub dobra interesu osoby fizycznej – z Systemów Rejestrów Państwowych lub złożonych oświadczeń, pism, przedstawionych dokumentów.
   np.:
   a. Wykonanie spisu uprawnionych do głosowania w wyborach powszechnych, na podstawie *Ustawy z dn. 5 stycznia 2011 Kodeks Wyborczy*, zawierają m.in. - Imię, Nazwisko, PESEL, Adres zamieszkania – dane są pobierane z rejestrów państwowych.

2. Realizacji zawartej umowy, dane niezbędne do jej realizacji – ze złożonych oświadczeń, pism i przedstawionych dokumentów.
   np.:

a. Wystawienie faktury za pobór wody i odprowadzenie ścieków, na podstawie zawartej umowy, dane pochodzące ze złożonych dokumentów, zawierają m.in. – Imię Nazwisko, adres zamieszkania, adres przyłącza.

3. Dobrowolnej zgody – za podstawie składanych oświadczeń, pism, przedstawianych dokumentów.
   np.:
   a. Składacie Państwo ofertę podjęcia pracy na rzecz gminy załączając CV, na podstawie Państwa zgody na przetwarzanie danych osobowych w postaci dołączonej lub zamieszczonej zgody w formie oświadczenia. Sami Państwo określacie zakres danych zawartych w tym dokumencie – choć niezbędne celem skomunikowania się, określenia Państwa personaliów, określenia kompetencji czy doświadczenia zawodowego.

Cel i podstawa prawna przetwarzania danych.
Urząd przetwarza dane osobowe realizując obowiązki wynikające z przepisów prawa, między innymi:

- ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych;
- ustawa z dnia 24 września 2010 r. o ewidencji ludności;
- ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej;
- ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami;
- ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego;
- ustawą z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych;
- ustawa z dnia 15 listopada 1984 r. o podatku rolnym;
- ustawa z dnia 7 września 1991 r. o systemie oświaty;
- ustawa z dnia 8 marca 1990 r. o samorządzie gminnym;
- ustawa z dnia 10 marca 2006 r. o zwrocie podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej;
- ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach;
- ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej;
- ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach;

oraz przepisami wykonawczymi do wymienionych ustaw.

Urząd realizuje również postanowienia umowne zawierane z osobami fizycznymi a dane osobowe przetwarzane są w ich zakresie wyłącznie do realizacji tych umów. np. umów na wywóz nieczystości.

Przetwarzane są również dane przekazywane dobrowolnie, w celu skontaktowania się z państwem w danej sprawie, udzielenia odpowiedzi lub w celach rekrutacji.

Rodzaj przetwarzanych danych.
Urząd przetwarza następujące dane: imiona, nazwiska, adresy, nr PESEL, imiona rodziców, nr dokumentów, nr telefonów, nr NIP, nr REGON, nr ewidencyjny, nr działek, adresy e-mail, adresy IP, wysokości podatków, wysokości opłat, wysokości wypłat, stan cywilny, stosunek do służby wojskowej, o ilości i imionach dzieci, o spełnianiu obowiązku szkolnego,

zatrudnienie, wykształcenie, zdjęcia, orzeczenia oraz decyzje administracyjne a także inne dane, wyłącznie niezbędne do realizacji poszczególnych zadań.

Prawa osoby której przetwarzane są dane.

1. Za przetwarzanie danych osób do 16 r.ż. odpowiadają opiekunowie prawni. Administrator ma prawo zweryfikować wiek osoby jeśli ma podejrzenia co do niespełnienia tego warunku.
2. Prawo do całkowitego usunięcia danych, przysługuje jeśli:
    a. Jeśli zauważycie Państwo że wasze dane są przetwarzane niezgodnie z prawem albo rodzaj przetwarzanych danych wykracza poza niezbędny zakres informacji;
    b. Jeśli dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego;
    c. Jeśli dane nie są już niezbędne;
    d. Jeśli cofniecie państwo zgodę na przetwarzanie danych osobowych, ale nie istnieje inna podstawa do ich przetwarzania;
3. Prawo do przenoszenia danych – można z niego skorzystać aby otrzymać od Administratora pełen zakres danych jaki Administrator zebrał na Państwa temat. Można z niego skorzystać jeśli dane przetwarzane są w ramach dobrowolnie wyrażonej zgody lub wynikają z zawartej umowy.
4. Prawo sprzeciwu wobec przetwarzanych danych osobowych wobec przekazania danych innemu administratorowi lub w celach marketingowych.
5. Prawo zmiany danych – możecie Państwo zmienić, zaktualizować swoje dane osobowe w każdym momencie, np. jeśli zmieniliście nazwisko, miejsce zamieszkania albo numer telefonu.

Jeśli Państwo uważają że dane przetwarzane przez urząd wykraczają ponad zakres wymagany do realizacji celu, czy skorzystać z przysługujących Państwu praw, należy się zgłosić do Inspektora Ochrony Danych.

Inspektor nie udziela szczegółowych odpowiedzi dotyczących Państwa danych osobowych przez telefon, zaś w przypadku zgłoszenia pisemnego skorzystania z Państwa praw lub obowiązku informacyjnego, pismo lub metoda kontaktu musi w sposób jednoznaczny określać, że to Państwo jesteście właścicielami tych danych osobowych.

Czas przechowywania danych.
Przetwarzane w urzędzie dane podlegają w większości przepisom ustawy o narodowym zasobie archiwalnym i archiwach i w zależności od rodzaju sprawy, dane te podlegają archiwizacji.

W przypadku danych wykorzystywanych poza obowiązkami wynikającymi z przepisów prawa, dane będą usuwane natychmiast po ustaniu realizacji celu w przypadku przetwarzania w formie papierowej, oraz minimum 2 lata maksymalnie 5 lat po ustaniu realizacji celu w przypadku przetwarzania w formie elektronicznej. Ten drugi wymóg wynika z zapewnienia rozliczalności zadań w systemach teleinformatycznych.

Udostępnianie danych osobowych.
Państwa dane osobowe mogą być przekazywane uprawnionym instytucjom reprezentujących interes publiczny na podstawie stosownych przepisów. Takimi instytucjami są między innymi:

Policja, sądy, wojsko, biura komornicze, ZUS, KRUS, szkoły i inne.
W przypadku przekazywania Państwa danych do innych podmiotów nierealizujących celu publicznego np. drukarnia wykonująca druki opłat z Państwa danymi, będziecie Państwo o tym fakcie poinformowani i do takiego celu będzie wymagane wyrażenie zgody.
Państwa dane mogą być przekazywane do innych krajów na podstawie stosownych przepisów i wyłącznie za pośrednictwem Ministerstwa Spraw Zagranicznych na jego wniosek.

Zabezpieczenie danych osobowych.
Państwa dane osobowe podlegają szczególnej ochronie. Aby zapewnić odpowiedni poziom bezpieczeństwa, w tutejszym urzędzie wdrożono Politykę Bezpieczeństwa Informacji oraz Instrukcję Zarządzania Systemem Informatycznym tworzące spójnie System Ochrony Danych. Dokumenty te są analizowane i na bieżąco aktualizowane aby przeciwdziałać nowo pojawiającym się zagrożeniom. Systemy informatyczne zabezpieczone są powszechnie uznawanymi metodami, zastosowano również rozwiązania organizacyjne i przeszkolono pracowników w zakresie ochrony danych osobowych.

Profilowanie i przetwarzanie automatyczne.
Tutejszy Urząd nie przetwarza danych automatycznie ani nie profiluje użytkowników.

Podstawa prawna i skargi.
Ochrona danych w urzędzie działa w oparciu o przepisy o ochronie danych osobowych w szczególności 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 powszechnie znanym pod nazwą RODO lub GDPR.

Macie Państwo prawo wnieść skargę w związku z przetwarzaniem przez nas Twoich danych osobowych do organu nadzorczego, którym jest Generalny Inspektor Ochrony Danych Osobowych

- Generalny Inspektor Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa

Załącznik nr 3
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

UMOWA

powierzenia przetwarzania danych osobowych,

zwana dalej Umową

zawarta w Zabłudowie w dniu …… r. pomiędzy:

Burmistrzem Zabłudowa z siedzibą w Zabłudowie, ur. Rynek 8, 16-060, reprezentowaną/ym przez:

……..…., zwaną/ym dalej Zleceniodawcą,
a
xxx z siedzibą w ……..…….., zarejestrowaną/ym w ..... pod numerem ....., posiadającą/ym numer NIP oraz numer REGON ……, reprezentowaną/ym przez: ....., zwaną/ym dalej Zleceniobiorcą

§ 1
Definicje

1. Podmiot przetwarzający – podmiot, któremu powierzono przetwarzanie danych osobowych na mocy umowy powierzenia ze Zleceniodawcą, zwany dalej Zleceniobiorcą

2. Administrator - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych, zwany także Zleceniodawcą

3. Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

4. Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

5. Rozporządzenie- 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),

6. Inny podmiot przetwarzający - podmiot, któremu podmiot przetwarzający w imieniu administratora pod-powierzył w całości lub częściowo przetwarzanie danych osobowych

§ 2
Przedmiot Umowy, cel, charakter i zakres

1. Przedmiotem umowy jest powierzenie przez Zleceniodawcę danych osobowych do przetwarzania przez Zleceniobiorcę.
2. Celem powierzenia jest: ……
3. Charakter przewarzania danych dotyczy przetwarzania danych osobowych w formie papierowej, przy wykorzystaniu systemów informatycznych.

§ 3
Czas trwania

1. Zleceniobiorca uprawniony jest do przetwarzania powierzonych danych do dnia wygaśnięcia lub rozwiązania Umowy.
2. W terminie 14 dni od ustania Umowy, Zleceniobiorca zobowiązany jest do usunięcia powierzonych danych, ze wszystkich nośników, programów i aplikacji w tym również kopii, chyba, że obowiązek ich dalszego przetwarzania wynika z odrębnych przepisów prawa.
3. Zleceniobiorca w terminie 14 dni od ustania Umowy zobowiązany jest do zwrotu powierzonych danych na nośnikach papierowych lub elektronicznych.

§4
Obowiązki i prawa

1. Zleceniobiorca zobowiązuje się współpracować ze Zleceniodawcą w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą.
2. Zleceniobiorca zobowiązuje się do pomocy Zleceniodawcy w wywiązaniu się z obowiązków określonych w art. 32-36 Rozporządzenia.
3. Zleceniobiorca zobowiązuje się do udostępnienia Zleceniodawcy wszelkich informacji niezbędnych do wykazania spełnienia obowiązków spoczywających na Zleceniobiorcy oraz umożliwi Zleceniodawcy lub audytorowi upoważnionemu przez Zleceniodawcę przeprowadzanie audytów, w tym inspekcji, współpracując przy działaniach sprawdzających i naprawczych.

§5
Zgłaszanie incydentów

1. Zleceniobiorca zobowiązuje się po stwierdzeniu naruszenia ochrony danych osobowych do zgłoszenia tego Zleceniodawcy bez zbędnej zwłoki.
2. Informacja przekazana Zleceniodawcy powinna zawierać co najmniej:
   a) opis charakteru naruszenia oraz - o ile to możliwe - wskazanie kategorii i przybliżonej liczby osób, których dane zostały naruszone i ilości/rodzaju danych, których naruszenie dotyczy
   b) opis możliwych konsekwencji naruszenia,
   c) opis zastosowanych lub proponowanych do zastosowania przez Zleceniobiorcę środków w celu zaradzenia naruszeniu, w tym minimalizacji jego negatywnych skutków.

§ 6

Korzystanie przez Zleceniobiorcę z usług innego podmiotu przetwarzającego

1. Zleceniobiorca w ramach realizacji Umowy korzysta z usług innego podmiotu przetwarzającego a Zleceniodawca przyjmuje to do wiadomości i wyraża na to zgodę.
2. W przypadku zmian dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, Zleceniodawca jest zobowiązany do poinformowania o tym Zleceniodawcę.
3. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Zleceniodawcy za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na Zleceniobiorcy.

§7

Deklarowane środki techniczne i organizacyjne

1. Zleceniobiorca gwarantuje, że każda osoba realizująca Umowę zobowiązana jest do bezterminowego zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy, a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym. Jednocześnie każda osoba realizująca Umowę zobowiązana jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.

2. Zleceniobiorca deklaruje stosowanie środków technicznych i organizacyjnych określonych w art. 32 Rozporządzenia, jako adekwatnych do zidentyfikowanego ryzyka naruszenia praw lub wolności powierzonych danych osobowych a w szczególności:
a. pseudonimizację i szyfrowanie danych osobowych;
b. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
c. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
3. Zleceniobiorca zobowiązuje się za pomocą odpowiednich środków technicznych lub organizacyjnych stosować ochronę powierzonych danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem (zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych) oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

§7a

Szczegółowe deklarowane środki techniczne i organizacyjne

Zleceniobiorca zobowiązuje się dopuszczać do przetwarzania danych osobowych osoby realizujące. Umowę poinformowane i przeszkolone z zasad bezpieczeństwa pracy z danych osobowymi.

1. Każda osoba realizująca Umowę zobowiązana jest do przetwarzania danych osobowych do których uzyskała dostęp wyłącznie w zakresie i celu przewidzianym w Umowie.
2. Każda osoba realizująca Umowę zobowiązana jest do zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym.
3. Każda osoba realizująca Umowę zobowiązuje się do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne.
4. Każda osoba realizująca Umowę zobowiązana jest do nie powodowania niezgodnych z Umową zmian danych lub utraty, uszkodzenia lub zniszczenia tych danych.
5. Każda osoba realizująca Umowę zobowiązuje się do niedokonywania jakiegokolwiek kopiowania i utrwalania danych osobowych poza systemami informatycznymi Zleceniodawcy
6. W przypadku wykorzystania sieci publicznej, każda osoba realizująca Umowę zobowiązuje się do stosowania zabezpieczonego przed podsłuchem połączenia zdalnego (VPN, SSL, podać inne).
7. Każda osoba realizująca Umowę zobowiązuje się do pracy w systemach Zleceniodawcy z użyciem uwierzytelnienia.

§8

Postanowienia końcowe

1. Umowa zastępuje wszelkie inne ustalenia dokonane pomiędzy Zleceniobiorcą a Zleceniodawcą dotyczące przetwarzania danych osobowych bez względu na to, czy zostały uregulowane umową czy innym instrumentem prawnym.
2. W zakresie nieuregulowanym Umową mają zastosowanie przepisy prawa obowiązującego na terenie Rzeczypospolitej Polskiej, w tym Rozporządzenia.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

....

(Zleceniodawca) (Zleceniobiorca)

Załącznik nr 4
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

Lp.	Nazwa Administratora	Opis kategorii przetwarzań (zakres usługi)	Kategoria osób których dane dotyczą	Numer umowy powierzenia
1				

Załącznik nr 5
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

P -Prawdopodobieństwo incydentu (skala od 1 do 3) **S-Skutki wystąpienia incydentu (skala od 1 do 3)** **R-Ryzyko wystąpienia incydentu (skala od 1 do 9)** **Formuła: R=P*S**	Informacje P / S / R		Programy, systemy operacyjne P / S / R		Infrastruktura IT P / S / R		Infrastruktura P / S / R		Pracownicy i współpracownicy P / S / R		Outsourcing P / S / R		ZABEZPIECZENIA	

Załącznik nr 6
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

……………………......………

(MIEJSCOWOŚĆ , DATA)

Nr: ……………………………………………

UPOWAŻNIENIE / ANULOWANIE UPOWAŻNIENIA
DO PRZETWARZANIA DANYCH OSOBOWYCH

Upoważniam		Anuluję upoważnienie	nr
Pana/Panią			
	imię	nazwisko	PESEL
Zatrudnionego na stanowisku:			

do przetwarzania danych osobowych w celach związanych z wykonywaniem powierzonych mu zadań służbowych. Upoważnienie dotyczy przetwarzania w systemach informatycznych oraz w formie papierowej następujących zbiorów i następującym zakresie:

Nazwa zbioru	Zakres czynności
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd

	❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie

Upoważnienie ma ważność do momentu cofnięcia go przez Administratora lub z dniem rozwiązania umowy o pracę.

....

Podpis Inspektora Ochrony Danych Podpis Administratora

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

WNIOSEK O NADANIE UPOWAŻNIENIA
DO PRZETWARZANIA DANYCH OSOBOWYCH

Proszę o nadanie upoważnienia

<table>
<tr><td rowspan="2">Panu/Pani</td><td></td><td></td><td></td></tr>
<tr><td>imię</td><td>nazwisko</td><td>PESEL</td></tr>
<tr><td colspan="2">Zatrudnionego na stanowisku:</td><td colspan="2"></td></tr>
</table>

do przetwarzania danych osobowych w celach związanych z wykonywaniem powierzonych mu zadań służbowych. Upoważnienie dotyczy przetwarzania w systemach informatycznych oraz w formie papierowej następujących zbiorów i następującym zakresie:

Nazwa zbioru	Zakres czynności
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie
	❑ Wgląd ❑ Wprowadzanie ❑ Modyfikacja ❑ Archiwizacja ❑ Udostępnianie innym podmiotom ❑ Usuwanie

.....
Podpis Kierownika Jednostki Organizacyjnej

Pracownik przeszedł szkolenie z zakresu ochrony danych osobowych

Dnia:

Wydano upoważnienie do przetwarzania danych osobowych

Nr/Dnia:

.....
Podpis Inspektora Ochrony Danych

Dokonano podłączenia do wskazanych zbiorów informatycznych

Dnia:

.....
Podpis Informatyka

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

Lp.	Wersja	Nazwa Procedury	Czego dotyczy	Data wprowadzenia	Data zniesienia

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

1. Rodzaj zabezpieczenia
    - Rozwiązanie 1
    - Rozwiązanie 2
    - Rozwiązanie n

2. Rodzaj zabezpieczenia
    - Rozwiązanie 1
    - Rozwiązanie 2
    - Rozwiązanie n

3. Rodzaj zabezpieczenia
    - Rozwiązanie 1
    - Rozwiązanie 2
    - Rozwiązanie n

4. Rodzaj zabezpieczenia
    - Rozwiązanie 1
    - Rozwiązanie 2
    - Rozwiązanie n

Załącznik nr 10
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

…… ……..

(imię i nazwisko) (miejscowość, data)

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz odnośnymi wymaganiami "Regulaminu Ochrony Danych Osobowych".

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach;
- zachowania w tajemnicy danych osobowych do których mam lub będę mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora;
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora;
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

Załącznik nr 11
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

Zakres szkolenia:

- Definicje dot. Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r., założenia rozporządzenia.
- Definicje dot. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, zmiany i założenia ustawy.
- Legalność przetwarzania danych osobowych – przesłanki legalności.
- Obowiązek informacyjny – z czego się składa i kiedy się go stosuje.
- Zasady ujawniania oraz powierzania danych osobowych – umowy powierzenia, podpowierzenie danych.
- Rejestr czynności przetwarzania
- Przepisy karne i odpowiedzialność.
- Przegląd zbiorów danych osobowych oraz programów służących do ich przetwarzania
- Przegląd treści Polityki Ochrony Danych Osobowych.
- Przegląd regulaminu ochrony danych osobowych w organizacji.
- Zabezpieczenia fizyczne obszarów przetwarzania.
- Zasady bezpiecznego użytkowania sprzętu IT
- Zasady bezpiecznego korzystania z oprogramowania.
- Zasady bezpiecznego korzystania z sieci Internet.
- Zasady bezpiecznego korzystania z poczty elektronicznej.
- Nadawanie upoważnień do przetwarzania danych osobowych.
- Instrukcja postępowania w przypadku wystąpienia incydentu.
- Postępowanie dyscyplinarne.

Załącznik nr 12
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

Zaświadczenie Nr rok/S/nr

Stwierdzające odbycie szkolenia z zakresu ochrony danych osobowych w świetle przepisów Ogólnego Rozporządzenia o Ochronie Danych oraz Regulaminu Ochrony Danych Osobowych w Urząd Miejski w Zabłudowie

Stwierdza się, że Pan(i):

Imię i nazwisko: **……..**

Data urodzenia: **…….**

Odbył(a) szkolenie z zakresu ochrony danych osobowych w świetle przepisów Ogólnego Rozporządzenia o Ochronie Danych oraz Regulaminu Ochrony Danych Osobowych, wymagane w Polityce Ochrony Danych Osobowych w Urząd Miejski w Zabłudowie, przeprowadzone przez Inspektora Ochrony Danych.

Zabłudów, …….. 2018r.

…….

Załącznik nr 13
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH ORAZ INCYDENTÓW BEZPIECZEŃSTWA DANYCH

nr incydentu	Data zgłoszenia	Opis / okoliczności naruszenia/incydentu	Ilość osób dotknięta naruszeniem/incydentem	Skutki naruszenia/incydentu	Działania zaradcze	Data rozpoczęcia wdrożenia działań	Data zakończenia wdrażania działań	Osoba odpowiedzialna za wdrożenie działań	Data zgłoszenia do organu nadzorczego
Nr/rok									
n									

Załącznik nr 14
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

opis	treść
rodzaj problemu	
czas zdarzenia	
czas wykrycia	
rodzaj działania	
źródło zdarzenia	
Osoba zgłaszająca	
Osoba odpowiedzialna	
Opis zdarzenia	
Opis szkód i zasięg (ilość potencjalnie poszkodowanych osób)	
Uwagi	

Załącznik nr 15
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

Protokół Nr ☐☐☐ / ☐☐☐☐ r.
ustalenia okoliczności i przyczyn naruszenia i incydentu Ochrony Danych

1. Nazwa Administratora danych osobowych

.....

nazwa lub imię i nazwisko Administratora Danych Osobowych

.....

adres siedziby Administratora Danych Osobowych

☐☐☐☐☐☐☐☐☐☐

NIP

2. Data, godzina oraz miejsce stwierdzenia naruszenia ochrony danych:

.....

3. Kategoria i ilość osób, których dotyczy naruszenie

.....

4. Zakres danych/kategorie danych których dotyczy incydent

.....

5. Osoba/źródło informacji o naruszeniu - kontakt

.....

Okoliczności naruszenia danych osobowych wraz z opisem charakteru naruszenia (analiza zdarzenia oraz przyczyny wydarzenia)
Opis skutków i konsekwencji naruszenia i incydentu
Podjęte działania – Opis środków jakie zostały lub zostaną podjęte w celu minimalizacji incydentu i jego negatywnych skutków

Osoba odpowiedzialna za wdrożenie działań naprawczych:

Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych? Jeżeli tak, to data i godzina przekazanej informacji, a w przypadku opóźnienia wyjaśnienie przyczyn opóźnienia zgłoszenia.

Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenia dotyczy? Jeżeli tak, to data i godzina oraz sposób przekazania informacji.

6. Podpisy Administratora danych osobowych oraz IOD

1) ..... 2) .....

czytelny podpis czytelny podpis

7. Protokół sporządzono dnia: .....

data

8. Wykaz załączników do protokołu:

Załącznik nr 16
do Polityki Bezpieczeństwa Danych Osobowych
dla Urzędu Miejskiego w Zabłudowie

Sprawdzenia i Audyty

Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.

1. Inspektor Ochrony Danych jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej.
2. Inspektor Ochrony Danych opracowuje programy audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
3. Inspektor Ochrony Danych wyznacza audytora do przeprowadzenia audytu.
4. Audytor jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów.
5. Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.
6. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia.
7. Wynik audytu zostaje udokumentowany przez audytora i przekazany Inspektorowi Ochrony Danych.
8. Inspektor Ochrony Danych dokonuje przeglądu i analizy wyniku audytu oraz w porozumieniu z Administratorem decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

Celem sprawdzenia jest wewnętrzna ocena wdrożonych systemów ochrony danych osobowych służąca do wykrycia nieprawidłowości i podatności celem ich eliminowania w drodze ulepszania systemu.

1. Inspektor Ochrony Danych jest odpowiedzialny za planowanie i przeprowadzanie sprawdzeń co najmniej raz w roku, jednak nie częściej niż co 3 miesiące.
2. Sprawdzeniu może podlegać jeden lub kilka wybranych systemów przetwarzania danych.
3. Inspektor Ochrony Danych opracowuje program sprawdzeń i informuje o nich odpowiedzialnych pracowników i kierownictwo nie wcześniej niż na 14 dni przed sprawdzeniem.
4. Po dokonaniu sprawdzenia, Inspektor Ochrony Danych prezentuje wyniki i zalecenia poprawy działania systemu administratorowi, który podejmuje decyzje w sprawie stosowania tych zaleceń.
5. Decyzje Administratora realizacji zaleceń są określane w ramach planu, który układa Inspektor Ochrony Danych, określane są cele do zrealizowania i termin wykonania zaleceń.