ZARZĄDZENIE NR 133/2020

BURMISTRZA ZIĘBIC

z dnia 21.09.2020r.

w sprawie

wprowadzenia Polityki Ochrony Danych Osobowych

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2020 r. poz. 713) i art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) zarządzam, co następuje:

§ 1.

W Urzędzie Miejskim w Ziębicach wprowadza się:

1. „Politykę Ochrony Danych Osobowych" co stanowi załącznik nr 1 do niniejszego zarządzenia;
2. „Regulamin Ochrony Danych Osobowych w Urzędzie Miejskim w Ziębicach", co stanowi załącznik nr 2 do niniejszego zarządzenia;
3. „Instrukcję zarządzania RODO w Urzędzie Miejskim w Ziębicach", co stanowi załącznik nr 3 do niniejszego zarządzenia;
4. „Politykę kluczy", co stanowi załącznik nr 4 do niniejszego zarządzenia;
5. „Procedurę postępowania z incydentami", co stanowi załącznik nr 5 do niniejszego zarządzenia;
6. „Procedurę realizacji praw osób, których dane dotyczą" co stanowi załącznik nr 6 do niniejszego zarządzenia;
7. „Regulamin funkcjonowania monitoringu wizyjnego w budynku Urzędu Miejskiego w Ziębicach", co stanowi załącznik nr 7 do niniejszego zarządzenia.

§ 2.

Zobowiązuję wszystkich pracowników Urzędu Miejskiego w Ziębicach do stosowania i przestrzegania dokumentacji o której mowa w § 1.

§ 3.

Traci moc zarządzenie Burmistrza Ziębic nr 99/2016 Burmistrza Ziębic z dnia 17 czerwca 2016 roku w sprawie wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miejskim w Ziębicach.

§ 4.

Wykonanie zarządzenia powierza się Sekretarzowi Gminy Ziębice.

§ 5.

Zarządzenie wchodzi w życie z dniem podjęcia.

BURMISTRZ ZIĘBIC
M. Szpilarewicz
Mariusz Szpilarewicz

RADCA PRAWNY
mgr Maciej Pływacz

Załącznik Nr 1 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09.2020 r

Polityka Ochrony Danych Osobowych

Spis treści

Załącznik Nr 1 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09 2020 r

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).
Administratorem przetwarzającym dane jest: Burmistrz Ziębic, z siedzibą w Urzędzie Miejskim w Ziębicach ul. Przemysłowa 10, 57-220 Ziębice.

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

1.1 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.

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

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.

Inspektor Ochrony Danych (Inspektor Ochrony Danych Osobowych, IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi, podmiotowi przetwarzającemu, 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.

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.

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.

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

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

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.

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

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

Profilowanie – jest dowolną formą 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.

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 (np. Listy referencyjnej nazwisk i numerów), 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.

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

Rejestr czynności przetwarzania danych – zestawienie czynności, które monitoruje w jaki sposób wykorzystuje się dane osobowe. Czynności te są wykonywane w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane. W rejestrze czynności przetwarzania danych zamieszcza się: nazwę czynności, cel przetwarzania, opis kategorii osób oraz danych, podstawę prawną przetwarzania, sposób zbierania ddanych, informację o przekazaniu danych poaz UE, sposób zbierania danych.

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. (Dz. Urz. UE L 119 z 04.05.2016).

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, które wyraża zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

1.2 Zakres Polityki

Polityka zawiera:

1. Opis zasad ochrony danych obowiązujących pracowników Urzędu Miejskiego w Ziębicach, którym kieruje Burmistrz Ziębic.
2. Odwołania do innych dokumentów wewnętrznych uszczegóławiających konkretne procedury, regulaminy lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach. Dokumenty wewnętrzne stają się obowiązujące z chwilą zatwierdzenia przez Administratora. Należy z nimi zapoznać każdą osobę upoważnioną do przetwarzania danych.

1.3 Odpowiedzialność za wdrożenie, utrzymanie i realizację Polityki

1. Za wdrożenie i zapewnienie przestrzegania Polityki odpowiedzialny jest Burmistrz Ziębic.
2. Osoba wyznaczona przez Burmistrza odpowiada za zapewnienie zgodności procedur i systemów informatycznych związanych z przetwarzaniem danych osobowych.
3. Inspektor Ochrony Danych odpowiada za monitorowanie przestrzegania Polityki.

1.4 Deklaracja Zgodności

Burmistrz Ziębic zapewnia zgodność przetwarzania danych osobowych z regulacjami RODO oraz krajowymi przepisami dotyczącymi ochrony danych osobowych - szczególnie w odniesieniu do: pracowników i klientów Urzędu Miejskiego w Ziębicach, a ponadto danych osobowych powierzonych do przetwarzania podmiotom trzecim.

2. Założenia ochrony danych

2.1 Filary ochrony danych osobowych

1. Legalność – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
2. Bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
3. Prawa osób – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4. Rozliczalność – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

2.2 Zasady ochrony danych

1. Burmistrz Ziębic wypełniając obowiązki prawne, w szczególności wynikające z ustawy z 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020r. Poz. 713), deklaruje, że dane są przetwarzane:
   1) w oparciu o podstawę prawną i zgodnie z prawem, na podstawie art. 6 i 9 RODO;
   2) rzetelnie

3) przez czas określony w przepisach

4) w konkretnych, wyraźnych i prawnie uzasadnionych celach

5) w sposób przejrzysty dla osoby, której dane dotyczą;

6) w zakresie niezbędnym w stosunku do celów przetwarzania;

7) z dbałością o prawidłowość danych;

8) z zapewnieniem odpowiedniego bezpieczeństwa danych.

2. Administrator w stosunku do osób których dane przetwarza wykonuje obowiązek informacyjny z uwzględnieniem art. 12, 13 i 14 RODO wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody).

3. Burmistrz Ziębic na podstawie art. 28 RODO zawiera umowy powierzenia z podmiotami przetwarzającymi. W tym celu prowadzi się wykaz podmiotów przetwarzających poprzez utworzenie Rejestru umów powierzenia.

2.3 System ochrony danych

System ochrony danych osobowych składa się z następujących elementów:

1. Inwentaryzacja danych - Administrator dokonuje identyfikacji zasobów przetwarzanych danych osobowych, kategorii danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
   - przypadków przetwarzania danych wrażliwych;
   - przypadków przetwarzania danych osób, których dane są niezidentyfikowane;
   - współadministrowania danymi.
2. Rejestr - Administrator opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych.
3. Umowy powierzenia przetwarzania danych - Administrator zawiera z podmiotami lub osobami, którym powierza przetwarzanie danych osobowych odpowiednie umowy, stosownie do art. 28 RODO.
4. Podstawy prawne - Administrator identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

   1) wprowadza system zarządzania zgodami na przetwarzanie danych i komunikację na odległość;

2) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy dane są przetwarzane na podstawie prawnie uzasadnionego interesu.

5. Obsługa praw jednostki - Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

   1) Administrator przekazuje wymagane prawem informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków (obowiązki informacyjne);

   2) Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania związanego z RODO przez siebie i swoich przetwarzających (możliwość wykonania żądań);

   3) Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane (obsługa żądań);

   4) Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych (zawiadamianie o naruszeniach).

6. Zasada prywatności w ustawieniach domyślnych (privact by default) - dane osobowe powinny być przetwarzane w zakresie, w którym są niezbędne dla osiągnięcia konkretnego celu. Obowiązek ten odnosi się w szczególności do:

   1) ilości zebranych danych osobowych;

   2) zakresu przetwarzanych danych osobowych;

   3) okresu przechowywania;

   4) dostępności do danych osobowych.

7. Bezpieczeństwo - Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

   1) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

   2) na podstawie art. 35 RODO przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

3) dostosowuje środki ochrony danych do ustalonego ryzyka;

4) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych – zarządza incydentami.

8. Zasada prywatności w fazie projektowania (Privacy by design) - Administrator zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów lub zadań uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności, zgodności celów przetwarzania, bezpieczeństwa danych już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

3. Ocena skutków (analiza ryzyka)

Administrator tworzy ocenę skutków, określoną w art. 35 RODO. Jest to procedura przeprowadzenia analizy ryzyka, która jest tworzona 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 jest stworzona na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

3.1 Opis operacji przetwarzania (inwentaryzacja aktywów)

1. W celu przeprowadzenia oceny skutków wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć.

2. Rejestr czynności w wersji do udokumentowania oceny skutków obejmuje takie informacje, jak:

a. opis kategorii osób;

b. opis celów przetwarzania;

c. charakter, zakres, kontekst danych osobowych;

d. odbiorcy danych;

e. funkcjonalny opis operacji przetwarzania;

f. aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing).

3.2 Analiza ryzyka

Procedura ta, 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 kategorii osób lub dla procesów przetwarzania.

Analiza ryzyka jest wykonywana dla kategorii osób i procesów przetwarzania poddanych ocenie skutków, jednak powinna być także przeprowadzana dla wszystkich istotnych kategorii osób zawartych w Rejestrze Czynności Przetwarzania, np. dla kategorii osób: kandydatów do pracy, pracowników, klientów.

3.3 Wyznaczenie zagrożeń i wyliczenie ryzyka dla 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.
3. Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania.
4. Skalę prawdopodobieństwa prezentuje Tabela A.
5. Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje czy skutki karne
6. Skalę skutków prezentuje Tabela B.
7. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: R=P*S.
8. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
9. Skalę Ryzyka prezentuje Tabela C.

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

Tabela C POZIOM RYZYKA	WARTOŚĆ [R = P*S]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

3.3.1. Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń.
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. Przeniesienie – przerzucenie ryzyka (outsourcing, ubezpieczenie);
    b. Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar miejsca pracy);
    c. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza miejsce pracy).
3. Analizę ryzyka przeprowadza się w specjalnym szablonie.

3.4 Plan postępowania z ryzykiem

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

4. Upoważnienia

1. Administrator odpowiada za nadawanie oraz anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienia dla pracowników nadawane są na wniosek przełożonych osób. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.
4. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO.

5. Środki organizacyjne i techniczne zabezpieczające dane osobowe

Administrator stosuje środki techniczne i organizacyjne (zabezpieczenia) adekwatne do zagrożeń naruszenia praw i wolności osób. W tym celu:

1. Administrator opracował i stosuje Regulamin Ochrony Danych Osobowych, Instrukcję zarządzania RODO, w których zabezpieczenia są opisane w formie procedur.
2. Dokumenty powinny być aktualizowane, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka (oceny skutków).
3. W celu zapewnienia wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania są opracowane procedury ochrony danych osobowych.
4. Pracownicy zostaną zaznajomieni ze stosowaniem środków organizacyjnych i technicznych.

6. Regulamin Ochrony Danych Osobowych

Regulamin Ochrony Danych Osobowych ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, poprzez podpisanie oświadczenia.

7. Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi powinna być przeszkolona i zapoznana z przepisami RODO.
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.
4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

8. Postępowanie z incydentami w zakresie naruszenia ochrony danych

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 zagrożeń lub wystąpieniu incydentu Inspektora Ochrony Danych.
2. Kontakt do w/w osoby w przypadku incydentu: tel. 74 8 163 870, email: iod@ziebice.pl.
3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;

3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

4. Do typowych incydentów bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);

2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata lub zagubienie danych);

3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

5. W przypadku stwierdzenia wystąpienia incydentu Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:

1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;

2) inicjuje ewentualne działania dyscyplinarne;

3) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;

4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

6. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

7. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

8. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

9. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

9. Rejestr Czynności Przetwarzania Danych (RCPD)

9.1 RCPD jako forma dokumentowania czynności przetwarzania danych osobowych

1. RCPD pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2. Administrator prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

3. RCPD jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych.

4. Pracownicy zatrudnieni na stanowiskach kierowniczych oraz samodzielnych zobowiązani są do zgłaszania IOD przypadków przetwarzania danych, ustania przyczyny przetwarzania uzasadniających wprowadzenie zmiany do RCPD, dążąc do tego aby wykazane były aktualne i odpowiadały rzeczywistej sytuacji.

5. W RCPD dla każdej czynności przetwarzania danych, która została uznała za odrębną dla potrzeb RCPD, należy odnotować co najmniej: (a) nazwę czynności, (b) cel przetwarzania, (c) opis kategorii osób, (d) opis kategorii danych, (e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu, (f) sposób zbierania danych, (g) opis kategorii odbiorców danych (w tym przetwarzających), (h) informację o przekazaniu poza UE (i) ogólny opis technicznych i organizacyjnych środków ochrony danych.

6. RCPD może zawierać także kolumny nieobowiązkowe, w których rejestruje się informacje dodatkowe ułatwiające zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

9.2. Podstawy przetwarzania

1. Administrator dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel) Administrator dookreśla podstawę w czytelny sposób, gdy jest to potrzebne, np.:

- dla zgody pracownika Urzędu Miejskiego w Ziębicach wskazując na jej zakres;
- gdy podstawą jest prawo - wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie;
- żywotne interesy - wskazując na kategorie zdarzeń, w których się zmaterializują;
- uzasadniony cel - wskazując na konkretny cel, np., dochodzenie roszczeń.

3. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

4. Pracownik Urzędu Miejskiego w Ziębicach ma obowiązek znać podstawy prawne, na jakich dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes, pracownik ma obowiązek znać konkretny realizowany przetwarzaniem interes.

10. Inspektor Ochrony Danych Osobowych

1. Status prawny i zadania Inspektora Ochrony Danych regulują przepisy Rozdziału IV Sekcji 4 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.

2. IOD w wykonywaniu swoich zadań podlega bezpośrednio Burmistrzowi.

3. Do zadań IOD należy w szczególności:

1) informowanie Burmistrza Ziębic oraz pracowników Urzędu Miejskiego w Ziębicach, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia

RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach;

2) monitorowanie przestrzegania rozporządzenia 2016/679, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

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

4) współpraca z organem nadzorczym;

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

4. Administrator zapewnia aby Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

11. Audyty

W celu oceny, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO Administrator określa poniższe zasady prowadzenia audytów.

1. IOD jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej.
2. IOD 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. Administrator niezależnie od działań IOD może przeprowadzić audyt w każdym czasie.
4. Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.

5. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, identyfikuje się tzw. uchybienia lub spostrzeżenia.
6. Audytor dokumentuje wyniki audytu i wraz z propozycją działań korygujących (przypadku zaistnienia poważnych uchybień) przekazuje Administratorowi.

12. Procedura przywrócenia dostępności danych osobowych i dostępu w razie incydentu fizycznego lub technicznego

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 2 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09.2020 r.

Regulamin Ochrony Danych Osobowych W Urzędzie Miejskim w Ziębicach

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników,
- Stażystów,
- Praktykantów,
- Współpracowników: m.in. osoby prowadzące jednoosobową działalność gospodarczą, wolontariusze
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający,
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający.

Na potrzeby niniejszego opracowania użyte w dalszej części określenie „użytkownik" odnosi się do w/w podmiotów.

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

Załącznik Nr 2 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09.2020 r.

Spis treści:

Załącznik Nr 2 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09.2020 r.

1 Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne instalowanie, otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do usuwania plików z nośników lub dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
5. Użytkownik jest zobowiązany do przekazania informatykowi Urzędu Miejskiego w Ziębicach nośników przeznaczonych do zniszczenia.
6. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa określonych dla komputerów przenośnych.

2 Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Każdy użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na wniosek przełożonych a wykonywane jest przez informatyka Urzędu Miejskiego w Ziębicach.
3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).
4. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.
6. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
7. Użytkownik jest zobowiązany do powiadomienia informatyka Urzędu Miejskiego w Ziębicach o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
8. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym informatyka Urzędu Miejskiego w Ziębicach.

9. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych wydziałów) wglądu do danych wyświetlanych na monitorach – tzw. polityka czystego ekranu.
10. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
11. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik działu informatyki. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
12. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;
    b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, magnetyczne i optyczne, na których znajdują się dane osobowe.

3 Zabezpieczenie dokumentacji papierowej z danymi osobowymi

1. Użytkownicy upoważnieni do przetwarzania danych osobowych są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Użytkownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu potrzebne do wykonywania w danym momencie pracy.
3. Użytkownik zobowiązany jest na bieżąco niszczyć te dokumenty, które przestały mu być potrzebne. Dokumenty powinny być niszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji w niszczarkach lub utylizacji ich według przyjętych procedur wewnętrznych.
4. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
5. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub pozostawiania ich na zewnątrz pomieszczenia pracy.
6. Obowiązuje zakaz trzymania na biurku wszelkich produktów spożywczych, które mogłyby zagrażać nośnikowi danych osobowych.

4 Polityka haseł

1. Hasła powinny składać się z minimum 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry lub znaki specjalne.

3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
6. Zmiana hasła następuje minimum co 30 dni.
7. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
8. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
9. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym organizacji.
10. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
11. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca. Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

5 Zasady wynoszenia nośników z danymi poza miejsce pracy

1. Użytkownicy nie mogą wynosić na zewnątrz budynku Urzędu Miejskiego w Ziębicach wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody bezpośredniego przełożonego. Do takich nośników zalicza się: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
2. Elektroniczne dane osobowe wynoszone poza budynek Urzędu Miejskiego w Ziębicach muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej np. w teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przenosi, przewozi pracownik, zobowiązany jest on do zabezpieczenia dokumentów przed zagubieniem i kradzieżą.
6. Zabrania się wynoszenia poza obszar Urzędu Miejskiego w Ziębicach wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi i pendrive bez zgody bezpośredniego przełożonego.
7. W sytuacji przekazywania nośników z danymi osobowymi poza obszar Urzędu Miejskiego w Ziębicach należy stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce;
    b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą;
    c. stosować bezpieczne koperty depozytowe;

d. przesyłkę należy przesyłać przez kuriera.

6 Zasady korzystania z Internetu

1. Pracownikom udostępnia się Internet jedynie do korzystania w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą informatyka i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych, pendrive, płyt CD, DVD i innych urządzeń dostępowych. Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci.

7 Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza organizację należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane w inny sposób do odbiorcy.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie wolno otwierać załączników typu .zip, .xlsm,, .exe w mailach. Zazwyczaj są to „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. Po otwarciu tych załączników istnieje wysokie ryzyko bezpowrotnej utraty danych.
7. Nie wolno otwierać hiperlinków w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik otwierając taki hiperlink infekuje komputer oraz inne komputery w sieci. Po otwarciu tych hiperlinków istnieje wysokie ryzyko bezpowrotnej utraty danych.
8. Należy zgłaszać informatykowi przypadki podejrzanych emaili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
11. Użytkownicy powinni okresowo kasować niepotrzebne maile.
12. Konta pocztowe służbowe są odseparowane od poczty prywatnej.
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
15. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
16. Przy korzystaniu z maila Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
17. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
18. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

8 Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

9 Zasady zabezpieczania kluczy

1. Administrator upoważnia użytkowników do pobierania kluczy do pomieszczeń.
2. Klucze do pomieszczeń szczególnie chronionych np. serwerowni, archiwum pozostają pod osobistym nadzorem osób upoważnionych. Dostęp osób trzecich do tych pomieszczeń odbywa się pod ścisłym nadzorem osób upoważnionych.
3. Klucze zapasowe przechowywane są w miejscu bezpiecznym wyznaczonym przez Sekretarza Gminy. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą osób uprawnionych. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu.
4. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
5. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
6. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
7. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń a w szczególności: wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi.

10 Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez pracodawcę zadaniach;
   b) zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez pracodawcę;
   c) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez pracodawcę;
   d) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
   e) 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.
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania danych odbywa szkolenie z zasad ochrony danych osobowych.

3. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
4. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
5. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania pracy w Urzędzie, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta Urząd oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.
6. Obowiązek zachowania w tajemnicy danych osobowych, które pracownik pozyskał w trakcie zatrudnienia w Urzędzie Miejskim w Ziębicach nie gaśnie wraz z rozwiązaniem stosunku pracy.

11 Zasady współpracy z IOD

1. Użytkownik zobowiązany jest do współpracy z IOD i udzielania mu pomocy w realizacji powierzonych zadań, w szczególności do:
   a) kontaktowania się z własnej inicjatywy z IOD w sprawach związanych z ochroną danych osobowych, w szczególności np.: zawieranie umów, realizowanie zadań własnych, projektowanie nowych rozwiązań;
   b) zgłaszania naruszeń;
   c) zgłaszania wniosków o realizację praw osób;
   d) zgłaszania wniosków o udostępnienie danych osobowych.

12 Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez pracodawcę za naruszenie przepisów karnych zawartych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (DZ. U. UE. L. Z 2016 r. Nr 119, str. 1 z późn. zm.).

Załącznik Nr 3 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09.2020r.

Instrukcja zarządzania RODO w Urzędzie Miejskim w Ziębicach

Załącznik Nr 3 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09.2020r.

Załącznik Nr 3 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09 2020r.

1. Wstęp

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.

2. Zabezpieczenia fizyczne

1. Zabezpieczono dostęp do kluczowej infrastruktury czyli pomieszczeń archiwów, serwerowni oraz miejsc przechowywania kopii bezpieczeństwa.
2. Wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej (praca personelu sprzątającego w godzinach pracy i w obecności osób upoważnionych).
3. Rozmieszczenie komputerów oraz kserokopiarek ogranicza dostęp osób nieupoważnionych.
4. Ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane gniazdka sieciowe (np. sale konferencyjne, korytarze).
5. Krytyczne elementy infrastruktury zabezpieczono w zamykanych na klucz szafach serwerowych.
6. Złącze główne zabezpieczono w szafach zamykanych na klucz.
7. Dostęp do pomieszczeń biurowych zabezpieczono drzwiami antywłamaniowymi oraz zamykanymi na klucz.
8. Dostęp do serwerowni zabezpieczono drzwiami zamykanymi na klucz oraz alarmem.
9. Dostęp do archiwum zabezpieczono drzwiami zamykanymi na klucz oraz alarmem.
10. Dokumentację zabezpieczono w zamkniętych na klucz niemetalowych szafach. Dokumentację pracowniczą zabezpieczono w zamkniętych na kod metalowych szafach.
11. Pomieszczenia chronione są przez system alarmowy oraz kraty.
12. Stosowana jest Polityka kluczy.

3. Zabezpieczenia techniczne

1. Redundantna linia zasilania.
2. Zastosowano UPS podtrzymujący zasilanie serwerowni.
3. Serwerownia wyposażona w gaśnice.
4. Serwerownia z materiałów niepalnych.
5. Czujnik przeciw pożarowy w serwerowni
6. Monitoring środowiskowy w serwerowni - czujnik temperaturowy oraz czujnik wilgotności.

7. Powiadamianie administratora systemu informatycznego o alertach temperatury oraz alertach wilgotności.
8. Klimatyzacja w serwerowni
9. Archiwum - składowanie dokumentacji papierowej na podwyższeniu

4. Procedura nadawania uprawnień do przetwarzania danych osobowych.

1. Dostęp do systemu informatycznego (programu, aplikacji oraz poczty elektronicznej) nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora.
2. Każdemu użytkownikowi uprzywilejowanemu (administratorowi) nadawane jest indywidualne konto administracyjne.
3. Nadawanie, zmiana, odbieranie uprawnień użytkownika do zasobów i aplikacji odbywa się na polecenie przełożonych lub innych osób upoważnionych.
4. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada informatyk w Urzędzie Miejskim w Ziębicach.
5. Powyższą procedurę wykonuje się poprzez przesłanie wniosku według załącznika o nadanie/ modyfikację/ odebranie zakresu uprawnień w systemie informatycznym e-maila przez Naczelnika wydziału Urzędu Miejskiego w Ziębicach do Informatyka Urzędu Miejskiego w Ziębicach z prośbą o dostęp do odpowiedniego wydziałowego katalogu. W tym przypadku stosuje się załączony wniosek o dostęp do uprawnień.
6. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
7. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.
8. W przypadku pracy z uprawnieniami użytkownika uprzywilejowanego, każdy Administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego "admin" dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.
9. Stosowany jest system uwierzytelniania Windowsa z wykorzystaniem loginu i hasła.

5. Metody i środki uwierzytelnienia (polityka haseł)

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez administratora i przekazywane mu w poufny sposób

2. Standard hasła: do komputera hasło min. 8-znakowe z użyciem dużych liter, małych liter, cyfr oraz znaków specjalnych. Zmiana hasła jest wymuszana przez system.
3. Administrator nie ma dostępu do haseł użytkowników.
4. W sytuacji zapomnienia przez użytkownika swojego hasła, administrator przywraca hasło do ustawień początkowych i przekazuje go użytkownikowi celem niezwłocznej późniejszej zmiany.
5. Zastosowano mechanizm blokady dostępu po 3 próbach nieudanego logowania się.
6. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
7. W przypadkach awaryjnych hasło może być przekazane decyzją Informatyka Urzędu Miejskiego w Ziębicach osobie zastępującej administratora
8. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła

6. Procedura tworzenia kopii zapasowych

1. Kopie zapasowe serwera (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany w oparciu o specjalne oprogramowanie oraz skrypt.
2. Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników w wybranym wydziałowym katalogu.
3. Kopie przyrostowe tworzy się codziennie o g. 1.00.
4. Kopie całościowe sporządzane są raz codziennie o g. 1.00.
5. Najstarsze kopie są nadpisywane w cyklu rotacyjnym co 36 miesięcy.
6. Kopie sporządzane są na wydzielonym serwerze NAS.
7. Co miesiąc sporządzana jest kopia serwera NAS na inny serwer.
8. Informatyk sprawuje nadzór nad poprawnością wykonania kopii zapasowych NAS
9. Niszczenie dysków z kopiami odbywa się komisyjnie. Nośniki niszczone są przez fizyczne zniszczenie po wymontowaniu z obudowy

7. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności macierze dyskowe, twarde dyski z danymi osobowymi ze stacji roboczych i laptopów, pendrive, pamięci flash, dyski SSD, płyty DVD, telefony komórkowe, smartfony są niszczone w sposób fizyczny w tym również komisyjnie według załącznika z protokółem zniszczenia uszkodzonych nośników. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników. Zniszczenie nośników można zlecić zewnętrznej jednostce. Zniszczenie musi być

potwierdzone protokołem zniszczenia, certyfikatem bezpieczeństwa lub nagraniem z procesu transportu i utylizacji.

2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar Urzędu Miejskiego w Ziębicach (np. sprzedaż lub darowizna komputerów stacjonarnych, laptopów, smartfonów).
3. Dokumentacja papierowa niszczona jest w niszczarkach ścinkowych.
4. Dokumentacja papierowa niszczona jest za zgodą Archiwum Państwowego według obowiązujących przepisów prawa. Brakowanie dokumentacji może odbywać się za pośrednictwem zewnętrznej jednostki zajmującej się niszczeniem dokumentacji.

8. Procedura zabezpieczenia systemu informatycznego

8.1. Bezpieczeństwo przetwarzania danych poza Urzędem Miejskim w Ziębicach

1. Użytkownicy komputerów przenośnych wynoszonych poza obszar Urzędu Miejskiego w Ziębicach na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa.
2. Stosuje się szyfrowanie bitlocker lub veracrypt dysków komputerów przenośnych zawierających dane osobowe, jeśli wynoszone są poza obszar Urzędu Miejskiego w Ziębicach.
3. Dane osobowe na komputerach przenośnych wynoszonych poza obszar Urzędu Miejskiego w Ziębicach muszą być przechowywane na zaszyfrowanych partycjach.
4. Dyski przenośne oraz pendrive wynoszone poza budynek Urzędu Miejskiego w Ziębicach muszą być zaszyfrowane.
5. Sprzęt mobilny (smartfony, tablety) zabezpieczono mechanizmem uwierzytelniania.
6. Sprzęt mobilny (komputery, laptopy, smartfony telefony komórkowe, tablety) wyposażony jest w oprogramowanie umożliwiające jego nadzór, blokowanie dostępu, czyszczenie zawartości.
7. W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet, stosuje się szyfrowanie tego połączenia z użyciem VPN przez Informatyka Urzędu Miejskiego w Ziębicach.
8. W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet uwierzytelnienia dokonuje się z użyciem loginu i podania hasła.

8.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

1. Dokonuje się aktualizacji oprogramowania firmware oraz sterowników urządzeń sieciowych oraz innych (w urządzeniach jak: routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery).
2. Dokonuje się konfiguracji urządzeń sieciowych oraz innych (routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery) w celu zabezpieczenia przed nieuprawnionym dostępem do nich np. zmiana domyślnych haseł na urządzeniach, zmiana domyślnych nazw kont administratora w urządzeniach, konfiguracja portów na routerze.
3. Dokonuje się aktualizacji oprogramowania systemów operacyjnych na stacjach roboczych, systemów operacyjnych serwerów, przeglądarek www, CMS, dedykowanego CMS, Adobe, Flash, Java. Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (aktualizacje, service pack-i, łatki)
4. Usługi sieciowe są monitorowane (DHCP, DNS, SSH, http, telnet, FTP, SMTP, SNMP) celem utrzymania niezbędnych usług a deaktywacji tych nieużywanych.
5. Zastosowano system antywirusowy na serwerze.
6. Zastosowano filtr antyspamowy.
7. Stosowany jest UTM sprzętowy.
8. Zastosowano mechanizmy kontroli dostępu do sieci w postaci: IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej oraz technikę NAT.
9. Zastosowano: Sewery proxy i bramki filtrujące (blokada ruchu na podstawie bazy reputacji, blokada dostępu do określonych stron).
10. Zastosowano inne mechanizmy monitorujące przeglądanie Internetu przez użytkowników: blokowanie stron internetowych określonego typu, blokowanie określonych stron internetowych, analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.
11. Sieć bezprzewodową zabezpieczono protokołem WEP oraz uwierzytelnianiem EAP.
12. Zastosowano specjalistyczne oprogramowanie monitorujące wymianę danych na styku sieci lokalnej i sieci rozległej.
13. Zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek.

8.3. Zabezpieczenia infrastruktury IT

1. Zastosowano wirtualizację serwera oraz redundantny serwer.
2. Zastosowano blokadę portów USB, DVD, CD na stacjach roboczych.
3. Zabezpieczono hasłem dostęp do portów fizycznych gniazd szeregowych, USB, Ethernet celem uniemożliwienia zmian konfiguracji przez osoby nieupoważnione.

4. Dokonano dezaktywacji nieużywanych gniazd sieciowych przez wypięcie przewodów lub wyłączenie portów na switchu.
5. Drukarki z funkcją kontroli wydruków.
6. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu", aktywowane po 3 minutach nieaktywności użytkownika
7. Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne

8.4. Zabezpieczenia aplikacji

1. Zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł oraz wyłączenie dostępu zdalnego, gdy nie jest wymagany.
2. Zabezpieczenie testowych wersji aplikacji poprzez zmianę domyślnych haseł oraz wyłączenie dostępu zdalnego, gdy nie jest wymagany.
3. Szyfrowanie baz danych.
4. W kluczowych aplikacjach stosuje się terminację sesji.
5. Stosuje się szyfrowanie poczty wychodzącej SSL.
6. Dla aplikacji webowych stosowane jest szyfrowanie połączeń internetowych z użyciem protokołu SSL, https.
7. Formularze kontaktowe na stronach www zabezpieczono protokołem SSL.
8. Zabezpiecza się logi systemowe przed sfałszowaniem.

9. Procedura wykonywania przeglądów i konserwacji

1. Stosowany jest system wykrywania słabości i zagrożeń (Skanery podatności).
2. Stosowane jest oprogramowanie do inwentaryzacji infrastruktury IT, zainstalowanego oprogramowania na stacjach roboczych i serwerach oraz do kontroli procesu aktualizacji (patche / łatki).
3. Stosowany jest system do monitoringu aktywności użytkowników.
4. Informatyk Urzędu Miejskiego w Ziębicach jest odpowiedzialny za monitoring, przegląd logów aktywności aplikacji, baz oraz uprawnień użytkowników i administratorów.
5. Informatyk Urzędu Miejskiego w Ziębicach odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków, optymalizację baz danych.
6. Informatyk Urzędu Miejskiego w Ziębicach odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email.
7. Informatyk Urzędu Miejskiego w Ziębicach odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia

8. W przypadku napraw dokonywanych na zewnątrz z komputerów należy uprzednio wymontować dyski i wszelkie nośniki, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania.
9. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z jednostek zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
10. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

Załącznik - Wniosek o nadanie/ modyfikację/ odebranie zakresu uprawnień w systemie informatycznym

Wniosek o nadanie/ modyfikację/ odebranie zakresu uprawnień w systemie informatycznym

Nowy użytkownik	Modyfikacja uprawnień	Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika:	Wydział:
Pomieszczenie:	Stanowisko:

Uprawnienia:	

Katalog Public	
Katalog Wydziału Ogólnego	
Katalog Wydziału Środowiska	
Katalog Referatu Spraw Mieszkaniowych	
Katalog Zespołu ds. Zamówień Publicznych	
Katalog Biura Rady	
Katalog Wydziału Gospodarki Nieruchomościami	
Katalog Wydziału Budownictwa	
Katalog Wydziału Funduszy Zewnętrznych i Promocji	
Katalog Urzędu Stanu Cywilnego	
Katalog Wydziału Finansowego	
Inne	

Programy:	
Efka 2000	
Finn	
Lex	
Bip	
Strona internetowa	
Geoportal (za zgodą Starostwa Powiatowego w Ząbkowicach Śl.)	
Giap	
E-mail	
Podpis elektroniczny	
Inne	

Uwagi:

Data i podpis bezpośredniego przełożonego:	
Data i podpis Informatyka:	Data i podpis IODO:

Załącznik Nr 2 do Instrukcji zarządzania RODO
w Urzędzie Miejskim w Ziębicach

..... dnia .....r.

Protokół nr .....
zniszczenia uszkodzonych nośników komputerowych
.....

Dnia ..... komisja powołana przez .....
(data) (imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:
1. Przewodniczący: .....
2. Członkowie: .....
.....
.....

dokonała trwałego zniszczenia nośników komputerowych:

L.p.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....
.....
.....
.....

Załącznik Nr 4 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09.2020 r

Polityka kluczy

1. Polityka kluczy obejmuje budynek Urzędu Miejskiego w Ziębicach przy ul. Przemysłowej 10.
2. Obowiązuje pięciodniowy tydzień pracy, od poniedziałku do piątku, w godzinach: w poniedziałek, środę, czwartek 07:30 – 15:30, wtorek 7:30-16:30, piątek 7:30-14:30.
3. Dostęp do pobierania kluczy do głównych drzwi Urzędu Miejskiego w Ziębicach mają wyłącznie osoby upoważnione przez Burmistrza Ziębic. Osoby posiadające klucze to:
   a) Burmistrz Ziębic – Mariusz Szpilarewicz
   b) Sekretarz Gminy – Rafał Śledź
   c) Konserwator – Adam Słoma
   d) Pracownik obsługi – robotnik gospodarczy – Renata Wiszniowska.
4. Dostęp do odblokowania alarmu do pomieszczeń szczególnie chronionych oraz głównych drzwi budynku Urzędu Miejskiego w Ziębicach mają wyłącznie osoby upoważnione przez Burmistrza Ziębic.

Nazwisko i imię	**Stanowisko**	**Pomieszczenie**
Szpilarewicz Mariusz	Burmistrz Ziębic	Wszystkie pomieszczenia
Śledź Rafał	Sekretarz Gminy	Wszystkie pomieszczenia
Huculak Sylwia	Kierownik Urzędu Stanu Cywilnego	Archiwum
Wrońska Mariola	Zastępca Kierownika Urzędu Stanu Cywilnego	Archiwum
Koba Gabriela	Podinspektor ds. finansowych - kasjer	Kasa
Dryk Dominika	Referent ds. administracyjno-organizacyjnych	Magazyn, Archiwum
Krawczyk-Łozińska Ewa	Inspektor ds. kadr i szkoleń	Archiwum
Lizis Marek	Informatyk	Wszystkie pomieszczenia
Słoma Adam	Konserwator	Główne drzwi Urzędu Miejskiego w Ziębicach

5. Po odkodowaniu alarmu przez upoważnionego pracownika, automatycznie wysyłana jest wiadomość sms do Burmistrza Ziębic, Sekretarza Gminy oraz Informatyka z informacją o użytym kodzie dostępu.
6. Klucze do pomieszczeń dla pracowników wydawane i zdawane są w sekretariacie Urzędu Miejskiego w Ziębicach.
7. Klucze zapasowe przechowywane są w sejfie w pokoju nr 13 Urzędu Miejskiego w Ziębicach. Wydawanie kluczy zapasowych może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą kierownika jednostki. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do sejfu.
8. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane (symbol wydziału oraz numer szafki).
9. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
10. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
11. Po zakończeniu pracy klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
12. Po zakończeniu pracy pracownicy są zobowiązani do zabezpieczenia pomieszczeń a w szczególności wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi.
13. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

Załącznik Nr 5do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09 2020 r

Procedura postępowania z incydentami

Spis treści

Załącznik Nr 5 do zarządzenia Nr 193/2020

Burmistrza Ziębic
z dnia 21.09.2020 r

1. Wstęp

Procedura opisuje sposób reagowania na naruszenia zagrażające bezpieczeństwu danych osobowych. Jej celem jest minimalizacja skutków wystąpienia naruszenia bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania zdarzeń w przyszłości.

1. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. W szczególności może to być:
   1) zdarzenie umyślne (np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń),
   2) zdarzenia losowe wewnętrzne (np. awaria komputera/serwera/dysku twardego/oprogramowania, pomyłki informatyków, utrata danych),
   3) zdarzenia losowe zewnętrzne (np. pożar, zalanie wodą, utrata zasilania, utrata łączności).

2. Postępowanie w przypadku naruszenia danych osobowych

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Inspektorowi Ochrony Danych Osobowych (IOD) poprzez wypełnienie formularza zgłoszenia.
2. Typowe sytuacje, które użytkownik powinien zgłosić IOD:
   1) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   2) dokumentacja jest niszczona bez użycia niszczarki,
   3) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
   4) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), zdjęciach, płytach CD w formie niezabezpieczonej itp,
   5) niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,
   6) ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
   7) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia,

8) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,
9) stwierdzenie próbę modyfikacji lub modyfikację danych, lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
10) telefoniczne próby wyłudzenia danych osobowych,
11) kradzież komputerów lub twardych dysków z danymi osobowymi,
12) utrata kontroli nad kopią danych osobowych,
13) e-maile zachęcające do ujawnienia identyfikatora i/lub hasła,
14) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
15) hasła do systemów przechowywane w pobliżu komputera.

3. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych, ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
4. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub innej osoby upoważnionej przez administratora danych.
5. Informatyk Urzędu Miejskiego w Ziębicach jest zobowiązany do informowania IOD o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem naruszenia
w zakresie danych osobowych.
6. IOD podejmuje następujące kroki:
   1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania, uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
   2) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
   3) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).
7. Polecenia IOD lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej procedury są priorytetowe i winny być wykonywane niezwłocznie, zapewniając ochronę danych podlegających ochronie.
8. IOD dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych, sporządzając raport.

9. IOD zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) wypełniając rejestr naruszeń i działań korygujących i zapobiegawczych.

3. Naruszenie danych osobowych– odpowiedzialność

Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującymi przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

4. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie, o którym mowa powyżej, musi co najmniej:
   1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych osobowych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
   3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
   4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli – i w jakim zakresie – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania przepisów RODO.

5. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych.
2. Zawiadomienie, nie jest wymagane, w następujących przypadkach:
   1) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   3) wymagałoby ono niewspółmiernie dużego wysiłku.

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

Załącznik Nr 1 do Procedury
postępowania z incydentami

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

Formularz zgłoszenia naruszenia Inspektorowi Ochrony Danych

Osoba powiadamiająca o naruszeniu oraz nazwa komórki organizacyjnej	
Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.) oraz data zdarzenia:	
Rodzaj naruszenia i określenie okoliczności mu towarzyszących:	
Podjęte działania:	

.....
(podpis pracownika)

.....
(podpis IOD)

Załącznik Nr 6 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09 2020 r.

Procedura realizacji praw osób, których dane dotyczą

Spis treści

Załącznik Nr 6 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09.2020 r.

1. Wstęp

1. Osobie, której dane dotyczą przysługują prawa na mocy art. 15-22 Rozporządzenia Parlamentu Europejskiego i Rady Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO): prawo dostępu do swoich danych, prawo do sprostowania danych, prawo usunięcia danych, prawo ograniczenia przetwarzania danych, prawo wniesienia sprzeciwu wobec przetwarzania danych, prawo do przenoszenia danych.
2. Osoba, której dane dotyczą może zwrócić się do Burmistrza Ziębic, jako Administratora jej danych osobowych o realizację przysługujących jej praw.
3. Ze względu na np. wykonywanie zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Burmistrzowi Ziębic, jako Administratorowi niektóre prawa osoby, o których mowa w art. 15-22 mogą nie mieć zastosowania lub mogą być ograniczone na podstawie Rozporządzenia Parlamentu Europejskiego i Rady Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) lub przepisów szczególnych.
4. Osoba, której dane dotyczą ma prawo uzyskać informację o nie podjęciu działań w związku z jej żądaniem lub o ograniczeniach w przysługujących jej prawach.
5. Osoba, której dane dotyczą, może zostać poproszona o dostarczenie dodatkowych informacji pozwalających ją zidentyfikować, jeżeli na podstawie posiadanych informacji nie ma możliwości potwierdzić jej tożsamość.

2. Prawo do informacji i kopii danych

Osoba, która chce się dowiedzieć, czy Administrator przetwarza dane na jej temat, może zwrócić się do Administratora o udzielenie informacji. Tego rodzaju wniosek nie wymaga uzasadnienia. Przepisy nie precyzują formy, w jakiej wniosek powinien być złożony, dlatego wniosek może przybrać formę dowolną; może to być wniosek pisemny, elektroniczny bądź zapytanie ustne. Administrator zobowiązany jest dokonać weryfikacji tożsamości osoby składającej wniosek, by upewnić się, że dane zostaną przekazane właściwej osobie. Wydanie kopii przetwarzanych danych wnioskującej osobie jest nieodpłatne, gdy jest to pierwszy wniosek, za kolejne kopie możliwa jest opłata.
Administrator bez zbędnej zwłoki - w terminie miesiąca od otrzymania żądania - powinien udzielić osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin

ten można przedłużyć o kolejne dwa miesiące, z uwagi na skomplikowany charakter żądania lub liczbę żądań.

W terminie miesiąca od otrzymania żądania, Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Uzyskanie informacji o spełnieniu żądania podmiotu danych, kończy postępowanie w tym zakresie. Uzyskanie informacji o niespełnieniu żądania, uprawnia podmiot danych do wniesienia skargi do organu nadzorczego zgodnie z art. 77 RODO.

3. Prawo do sprostowania danych

Osoba której dane dotyczą, ma prawo do żądania dokonania korekty, bądź usunięcia jej danych, jeśli są one nieprawdziwe, niepełne lub zostały zebrane w sposób sprzeczny z ustawą. Unijne rozporządzenie o ochronie danych nakłada na Administratora obowiązek zapewnienia prawidłowości danych. Dane osobowe powinny być prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

W przypadku rozbieżności między stanem faktycznym, a treścią danych, prawodawca unijny przyznał osobie, której dane dotyczą, uprawnienie do żądania od Administratora sprostowania przetwarzanych danych, a w przypadku, gdy dane są niekompletne, podmiot danych może domagać się ich uzupełnienia. Ciężar wykazania nieprawidłowości spoczywa na osobie, której dane dotyczą.

4. Prawo do bycia zapomnianym

W określonych w rozporządzeniu przypadkach prawodawca unijny przyznał osobie, której dane dotyczą, uprawnienie do żądania od Administratora usunięcia danych jej dotyczących. Uprawnienie to, określane jest także mianem „prawa do bycia zapomnianym".

Jeżeli osoba, której dane dotyczą:

- stwierdzi, że dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
- cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
- wnosi sprzeciw wobec przetwarzania jej danych i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
- stwierdzi, że dane osobowe były przetwarzane niezgodnie z prawem,
- stwierdzi, że dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega Administrator,
- stwierdzi, że dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego,

to może zwrócić się do Administratora z żądaniem usunięcia danych. Ciężar dowodu (wykazania nieprawidłowości, nielegalności przetwarzania bądź zbędności danych) ciąży na osobie, której dane dotyczą.

5. Prawo do ograniczenia przetwarzania

Przepisy RODO przewidują uprawnienie osoby, której dane dotyczą, do żądania od Administratora ograniczenia ich przetwarzania.
Jeżeli osoba, której dane dotyczą:

- kwestionuje prawidłowość danych, może zwrócić się do Administratora z żądaniem ograniczenia przetwarzania danych - na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych,
- sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystania, gdy przetwarzanie jest niezgodne z prawem,
- stwierdza, że dane są jej potrzebne do ustalenia, dochodzenia lub obrony roszczeń, a Administrator nie potrzebuje już danych osobowych do celów przetwarzania,
- wniosła sprzeciw – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.

6. Prawo do przenoszenia danych

W przypadku, gdy przetwarzanie danych osobowych odbywa się w sposób zautomatyzowany, tzn. jeżeli czynności, które są wykonywane w ramach procesów przetwarzania, realizowane są przez systemy informatyczne lub inne mechanizmy pozwalające na automatyzację (wykonywanie czynności przez maszynę samoczynnie, bez każdorazowego działania człowieka), osoba, której dane dotyczą, może zwrócić się do Administratora z wnioskiem o przeniesienie danych osobowych. Dla możności skorzystania z prawa do przenoszenia danych prawodawca unijny wymaga łącznego spełnienia przesłanek dotyczących: podstawy przetwarzania (zgoda lub umowa) oraz sposobu przetwarzania (zautomatyzowany).

7. Prawo do sprzeciwu

Jeżeli osoba, której dane dotyczą, sprzeciwia się przetwarzaniu danych na swój temat, może wnieść do Administratora sprzeciw. Sprzeciw nie przysługuje jednak w przypadku, gdy osoba wyraziła zgodę na przetwarzanie danych. Jeżeli osoba nie chce, aby Administrator dalej przetwarzał jej dane, powinna cofnąć zgodę.
Sprzeciw nie przysługuje również w przypadku, gdy:

- podstawą przetwarzania danych osobowych jest konieczność realizacji umowy (art. 6 ust. 1 lit. b RODO);
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze (art. 6 ust. 1 lit. c RODO);
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d RODO).

8. Informacje o prawie wniesienia skargi do organu nadzorczego

Bez uszczerbku dla innych Administracyjnych lub środków ochrony prawnej przed sądem, każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza rozporządzenie RODO. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 78 RODO. Każda osoba fizyczna ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna iż przetwarzanie danych osobowych jej dotyczących narusza przepisy RODO.

W celu skorzystania z przysługujących praw osoba której dane dotyczą powinna dostarczyć do Administratora wniosek:
Osobiście / pisemnie: Urząd Miejski w Ziębicach, ul. Przemysłowa 10, 57-220 Ziębice
Elektronicznie: e-mail na adres iod@ziebice.pl
Za pośrednictwem ePuap przy wykorzystaniu np. wzoru „pismo ogólne do podmiotu publicznego"

9. Terminy i sposób załatwienia sprawy

Zgodnie z art. 12 ust. 3 rozporządzenia 2016/679 bez zbędnej zwłoki, nie dłużej jednak niż w terminie miesiąca od otrzymania żądania. W przypadku skomplikowanego charakteru sprawy (charakter żądania lub liczba żądań) termin ten można przedłużyć o kolejne dwa miesiące.

Zgodnie z art. 12 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) Administrator bez zbędnej zwłoki - w terminie miesiąca od otrzymania żądania - powinien udzielić osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące, z uwagi na skomplikowany charakter żądania lub liczbę żądań.

W terminie miesiąca od otrzymania żądania, Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Uzyskanie informacji o spełnieniu żądania podmiotu danych kończy postępowanie w tym zakresie. Uzyskanie informacji o niespełnieniu żądania, uprawnia podmiot danych do wniesienia skargi do organu nadzorczego zgodnie z art. 77 RODO. Administrator może odmówić podjęcia działań w związku z żądaniem w przypadku kiedy żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione, nadmierne, w szczególności na swój ustawiczny charakter.

10. **Tryb odwoławczy**

W przypadku nie podjęcia działań w związku z żądaniem osoby, której dane dotyczą Administrator informuje osobę, której dane dotyczą, o powodach nie podjęcia działań oraz o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem.

11. Podstawa prawna

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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. Urz. UE L 119 z 04.05.2016, str. 1), zwanym wyżej "rozporządzeniem 2016/679", RODO.

Załącznik Nr 1 do Procedury realizacji praw osób,
których dane dotyczą

.....
(miejscowość, data)

Wniosek osoby, której dane dotyczą

Burmistrz Ziębic
Ul. Przemysłowa 10
57-220 Ziębice

Imię i nazwisko wnioskodawcy	
Adres zamieszkania	
PESEL	
Dane kontaktowe (Tel. e-mail)	
Zakres żądania:	a) dostęp do danych osobowych, b) sprostowanie danych osobowych, c) ograniczenie przetwarzania danych osobowych, d) wniesienie sprzeciwu wobec przetwarzania danych osobowych, e) przeniesienie danych osobowych, f) cofnięcia zgody na przetwarzanie danych osobowych (*jeżeli przetwarzanie będzie odbywać się na podstawie zgody),* g) usunięcie danych osobowych („prawo do bycia zapomnianym").
Jakich danych wniosek dotyczy	
Jeżeli to możliwe, prosimy o wskazanie rodzaju świadczonej na Pani/Pana rzecz usługi lub innej informacji związanej z przetwarzaniem Pani/Pana danych przez naszą Urząd. **Prosimy określić możliwe daty lub ramy czasowe, w których dane zostały nam przekazane, jak również rodzaje dokumentów na których dane zostały podane np. umowy, lub wszelkie inne informacje, które umożliwią nam zlokalizowanie Pani/Pana danych.**	

Ja niżej podpisany, potwierdzam, że informacje podane w niniejszym wniosku są prawidłowe oraz że jestem osobą, której dane dotyczą, i której dane zostały podane w niniejszym formularzu. Przyjmuję do wiadomości, że Administrator musi potwierdzić moją tożsamość i dlatego może zaistnieć konieczność ponownego skontaktowania się ze mną w celu uzyskania dalszych informacji potrzebnych do potwierdzenia tożsamości lub zlokalizowania danych osobowych, o które wnioskuję. Rozumiem, że mój wniosek nie będzie skuteczny, dopóki nie przekażę wszystkich potrzebnych informacji do jego rozpatrzenia i przygotowania odpowiedzi.

.....
(data i podpis wnioskodawcy)

Załącznik Nr 7 do zarządzenia Nr 193/2020
Burmistrza Ziębic
z dnia 21.09.2020 r.

Regulamin funkcjonowania monitoringu wizyjnego w budynku Urzędu Miejskiego w Ziębicach

§ 1

1. Regulamin określa zasady działania monitoringu wizyjnego w budynku Urzędu Miejskiego w Ziębicach oraz na parkingu przed budynkiem. Regulamin określa również cele oraz stosowane środki techniczno-organizacyjne zapewniające bezpieczne rejestrowanie i usuwanie nagrań, miejsca instalacji kamer, sposób udostępniania nagrań.
2. Administratorem przetwarzającym dane jest: Burmistrz Ziębic, z siedzibą w Urzędzie Miejskim w Ziębicach ul. Przemysłowa 10, 57-220 Ziębice.

§ 2

1. Celem stosowania monitoringu wizyjnego w Urzędzie Miejskim w Ziębicach jest:
   a) zapewnienie bezpieczeństwa osobom przebywającym na terenie budynku Urzędu Miejskiego w Ziębicach;
   b) zapewnienie ochrony mienia oraz bezpieczeństwa pomieszczeń.
2. System monitoringu wizyjnego obejmuje zestaw kamer, rejestrator, oprogramowanie do obserwacji zapisów.
3. Monitoring funkcjonuje całą dobę.
4. Rejestracji i zapisywaniu na nośniku fizycznym podlega obraz z kamer systemu monitoringu.
5. Administrator oznacza miejsce objęte monitoringiem w sposób widoczny i czytelny.
6. Miejsca objęte monitoringiem są oznakowane tabliczkami informacyjnymi, które powinny zawierać:
   a) informację o administratorze danych;
   b) piktogram informujący o monitoringu danego miejsca;
   c) pełną treść obowiązku informacyjnego na podstawie art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119 z 04.05.2016, dalej RODO) dostępną w Sekretariacie Urzędu Miejskiego w Ziębicach;
   d) wzór tabliczki informacyjnej oraz treść obowiązku informacyjnego stanowi odpowiednio Załącznik nr 1 i 2 do niniejszego Regulaminu.
7. Nadzór nad funkcjonowaniem systemu monitoringu sprawuje Informatyk Urzędu Miejskiego w Ziębicach.
8. Dostęp do odtwarzania zarejestrowanego obrazu z monitoringu wizyjnego i wykorzystania go do działań wewnętrznych posiada Administrator lub osoby przez niego upoważnione.

9. Do zapoznania się z nagraniami z monitoringu upoważnieni na podstawie art. 29 RODO są:
   a) Sekretarz Gminy;
   b) Informatyk Urzędu Miejskiego w Ziębicach;
   c) Inspektor Ochrony Danych Osobowych
10. Monitoringiem objęte są :
   a) budynek Urzędu Miejskiego w Ziębicach przy ul. Przemysłowej 10, 57-220 Ziębice:
   - Kamera nr 1 – Korytarz wejściowy (kamera skierowana na wejście do kasy);
   - Kamera nr 2 – Kasa w pokoju nr 6;
   - Kamera nr 3 – Korytarz na pierwszym piętrze (kamera skierowana na wejście do sekretariatu).
   b) Kamera nr 4 i 5 skierowana na parking przed budynkiem Urzędu Miejskiego w Ziębicach.
11. Rejestrator wraz z podglądem do monitoringu zamontowany jest w serwerowni Urzędu Miejskiego w Ziębicach.

§ 3

1. Administrator jest zobowiązany zapewnić odpowiednie środki techniczne i organizacyjne, aby żadna osoba nieuprawniona nie miała dostępu do urządzeń oraz nagrań zarejestrowanych za pomocą tych urządzeń.
2. Administrator jest zobowiązany do tego aby zapewnić bezpieczne przechowywanie nagrań od momentu ich zarejestrowania do momentu ich usunięcia.
3. Zapisy monitoringu przechowywane są przez 30 dni od dnia nagrania. W przypadku gdy zarejestrowany obraz może być użyty lub będzie użyty jako dowód w postępowaniu prowadzonym przez właściwy sąd lub inny organ publiczny administrator zobowiązany jest do przechowywania nagrania do czasu zakończenia postępowania.
4. Po upływie terminu, o którym mowa w ust. 3 administrator jest zobowiązany za zniszczenie materiałów z monitoringu wizyjnego.
5. Dysk twardy przechowujący zarejestrowany obraz przeznaczony do:
   a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   b) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 4

1. Administrator poprzez realizację prawa dostępu do danych osób, których dane dotyczą jest zobowiązany do udostępnienia danych pod warunkiem, że zostanie dokonana anonimizacja wizerunku osób, których żądanie nie dotyczy.

2. Administrator może odstąpić od obowiązku anonimizacji wizerunku osób, których żądanie nie dotyczy gdy uzna, że interes osoby, która wystąpiła z żądaniem jest nadrzędny wobec praw innych osób zarejestrowanych na nagraniu.
3. Anonimizacja jest przeprowadzana z wykorzystaniem programu
4. Administrator lub osoba przez niego upoważniona weryfikuje poprawność anonimizacji.
5. Administrator lub osoba przez niego upoważniona udostępnia w trybie przeglądania nagranie.

§ 5

1. Pracodawca jest zobowiązany do poinformowania wszystkich pracowników o celu i sposobie stosowania monitoringu wizyjnego.
2. Przekazanie tej informacji dotyczących monitoringu wizyjnego następuje na piśmie poprzez podpisanie oświadczenia. Wzór oświadczenia stanowi Załącznik nr 3.
3. W sprawach nieuregulowanych niniejszym regulaminem, ostateczną decyzję podejmuje Administrator.

INFORMACJA O MONITORINGU

- administratorem systemu monitoringu jest Burmistrz Ziębic z siedzibą w Urzędzie Miejskim w Ziębicach przy ul. Przemysłowej 10, 57-220 Ziębice
- monitoring stosowany jest celu ochrony mienia oraz zapewnienia bezpieczeństwa na terenie monitorowanym
- podstawą przetwarzania jest art. 22^2 Kodeksu pracy (Dz. U. z 2020 r. poz. 1320) oraz art. 111 Ustawy o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781)
- zapisy z monitoringu przechowywane będą przez 30 dni
- osoba zarejestrowana przez system monitoringu ma prawo do dostępu do danych osobowych
- osobie zarejestrowanej przez system monitoringu przysługuje prawo wniesienia skargi do organu nadzorczego
- kontakt do Inspektora Ochrony Danych Osobowych: email: iod@ziebice.pl

Załącznik nr 2 do Regulamin funkcjonowania
monitoringu wizyjnego w budynku
Urzędu Miejskiego w Ziębicach

MONITORING WIZYJNY – klauzula informacyjna

Zgodnie z art. 13 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 (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), informujemy o zasadach przetwarzania Pani/Pana danych osobowych oraz o przysługujących Pani/Panu prawach z tym związanych:

1. Administratorem Pani/Pana danych osobowych w Urzędzie Miejskim jest Burmistrz Ziębic z siedzibą przy ul. Przemysłowa 10, 57-220 Ziębice, tel. 74 8 163 870, fax: 74 8 191 212, e-mail: urzad@ziebice.pl.
2. Administrator wyznaczył Inspektora ochrony danych, z którym możliwy jest kontakt w sprawie danych osobowych: listowny na wyżej wskazany adres korespondencyjny bądź e-mailowy: iod@ziebice.pl.
3. Pani/Pana dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. c. RODO (wypełnienie obowiązku prawnego ciążącego na administratorze) w związku z art. 22^2 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy.
4. Pani/Pana dane osobowe będą przetwarzane w celu zapewnienia bezpieczeństwa pracowników Urzędu Miejskiego w Ziębicach oraz ochrony mienia.
5. Monitoring wizyjny obejmuje korytarze budynku Urzędu Miejskiego w Ziębicach oraz kasę.
6. Odbiorcami Pani/Pana danych osobowych mogą być podmioty, które przetwarzają dane osobowe w imieniu Administratora na podstawie zawartej z administratorem umowy powierzenia przetwarzania danych osobowych.
7. Zapisy z monitoringu przechowywane są przez okres 30 dni od dnia nagrania. W przypadku gdy zarejestrowany obraz może być użyty lub będzie użyty jako dowód w postępowaniu prowadzonym przez właściwy sąd lub inny organ publiczny administrator zobowiązany jest do przechowywania nagrania do czasu zakończenia postępowania.
8. Zapis z monitoringu może zostać udostępniony właściwym organom w zakresie realizowanych przez nie zadań ustawowych. Dane mogą zostać udostępnione na podstawie pisemnego wniosku w związku z prowadzonym postępowaniem.
9. Posiada Pan/i prawo żądania dostępu do swoich danych osobowych, sprostowania (poprawiania), usunięcia lub ograniczenia przetwarzania, a także sprzeciwu na przetwarzanie, przy czym przysługuje ono jedynie w sytuacji, jeżeli dalsze przetwarzanie nie jest niezbędne do wywiązania się przez Administratora z obowiązku prawnego i nie występują inne nadrzędne prawne podstawy przetwarzania.
10. Przysługuje Pani/u prawo do wniesienia skargi na realizowane przez Administratora przetwarzanie Pani/a danych do Prezesa UODO (Stawki 2, 00-193 Warszawa, www.uodo.gov.pl).

Załącznik nr 3 do Regulamin funkcjonowania
monitoringu wizyjnego w budynku
Urzędu Miejskiego w Ziębicach

Oświadczenie pracownika o zapoznaniu się z zasadami stosowania monitoringu wizyjnego w Urzędzie Miejskim w Ziębicach

Niniejszym informuję, na podstawie art. 22^2 ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy, że na terenie Urzędu Miejskiego w Ziębicach funkcjonuje monitoring wizyjny.

Monitoringiem w Urzędzie Miejskim w Ziębicach objęte są:

- Korytarz wejściowy (kamera skierowana na wejście do kasy);
- Kasa w pokoju nr 6;
- Korytarz na pierwszym piętrze (kamera skierowana na wejście do sekretariatu).

oraz parking przed budynkiem Urzędu Miejskiego w Ziębicach.

Celem działania monitoringu wizyjnego jest zwiększenie bezpieczeństwa pracowników oraz ochrona mienia.

Oświadczam, że zostałam/em poinformowany o celach, zakresie i sposobie funkcjonowania monitoringu wizyjnego w Urzędzie Miejskim w Ziębicach.

.....

(data i czytelny podpis pracownika)