SM.142.1.2021 Ziębice, 30.03.2021 r.

Wprowadzenie Polityki Ochrony Danych Osobowych w Straży Miejskiej w Ziębicach

Na podstawie art. 10a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (t.j. Dz. U. z 2019 r. poz. 1795 z późn. zm.) i art. 31 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) w Straży Miejskiej wprowadza się:

1. „Politykę Ochrony Danych Osobowych", co stanowi załącznik nr 1 do niniejszego dokumentu;
2. „Regulamin Ochrony Danych Osobowych w Straży Miejskiej w Ziębicach", co stanowi załącznik nr 2 do niniejszego dokumentu;
3. „Instrukcję zarządzania RODO w Straży Miejskiej w Ziębicach", co stanowi załącznik nr 3 do niniejszego dokumentu;
4. „Procedurę postępowania z incydentami", co stanowi załącznik nr 4 do niniejszego dokumentu;
5. „Procedurę realizacji praw osób, których dane dotyczą", co stanowi załącznik nr 5 do niniejszego dokumentu;
6. „Politykę czystego biurka i ekranu w Straży Miejskiej w Ziębicach" co stanowi załącznik nr 6 do niniejszego dokumentu;
7. „Politykę kluczy", co stanowi załącznik nr 7 do niniejszego dokumentu.

Wszyscy pracownicy Straży Miejskiej w Ziębicach oraz pracownicy Urzędu Miejskiego w Ziębicach, którzy przetwarzają dane na podstawie ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), są zobowiązani do stosowania i przestrzegania dokumentacji, o której mowa powyżej.

Komendant
Straży Miejskiej w Ziębicach
Radosław Wolny

Załącznik Nr 1

Polityka Ochrony Danych Osobowych w Straży Miejskiej w Ziębicach

Spis treści

1. Wstęp....2
   1.1 Definicje....2
   1.2 Zakres Polityki....5
   1.3 Odpowiedzialność za wdrożenie, utrzymanie i realizację Polityki....5
   1.4 Deklaracja Zgodności....5
2. Założenia ochrony danych....6
   2.1 Filary ochrony danych osobowych....6
   2.2 Zasady ochrony danych....6
   2.3 System ochrony danych....7
3. Szacowanie ryzyka i ocena skutków....9
   3.1 Szacowanie ryzyka....9
   3.2 Ocena skutków....10
   3.3 Wyznaczenie zagrożeń i wyliczenie ryzyka dla zagrożeń....10
   3.4 Plan postępowania z ryzykiem....13
4. Upoważnienia....14
5. Środki organizacyjne i techniczne zabezpieczające dane osobowe....14
6. Regulamin Ochrony Danych Osobowych....14
7. Szkolenia....15
8. Postępowanie z incydentami w zakresie naruszenia ochrony danych....15
9. Rejestr Czynności Przetwarzania Danych (RCPD)....17
   9.1 RCPD jako forma dokumentowania czynności przetwarzania danych osobowych....17
   9.2. Podstawy przetwarzania....18
10. Inspektor Ochrony Danych Osobowych....18
11. Audyty....19
12. Procedura przywrócenia dostępności danych osobowych i dostępu w razie incydentu fizycznego lub technicznego....20

Załącznik Nr 1

1. Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych, które są stosowane przez Administratora w celu spełnienia wymagań Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.) (dyrektywa policyjna) oraz Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

Administratorem przetwarzającym dane jest: **Komendant Straży Miejskiej w Ziębicach,** z siedzibą przy Placu Strażackim 8, 57-220 Ziębice.

Polityka stanowi jeden ze środków organizacyjnych, mających na celu realizację czynności związanych z przetwarzaniem, zapobieganiem, wykrywaniem i zwalczaniem czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności, uwzględniając jednocześnie wyłączenia, o których mowa w art. 3 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), a szczególnie wyłączenia w przedmiocie Ustawy z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia (t.j. Dz. U. z 2021 r. poz. 457).

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 albo jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego.

DODO - Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WsiSW (Dz. U. UE. L. Z 2016r., Nr 119, str 89 z późn. zm.). – dyrektywa policyjna.

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, których dane są przetwarzane oraz dla 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. Ocena skutków powinna być przeprowadzona przed przetwarzaniem danych, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób. Powinna być wykonana również gdy przetwarzanie 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 ochronie przez środki techniczne i organizacyjne w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szacowanie ryzyka – całościowy proces, który dotyczy: identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka. Analiza ryzyka to proces dążący do poznania charakteru danych oraz określenia poziomu ryzyka. Ocena ryzyka to proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane.

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 danych, informację o przekazaniu danych poza UE, sposób zbierania danych.

Rozliczalność – dotyczy zapewnienia zgodności ze wszystkimi zasadami przetwarzania, bez względu na sposób, w jaki dane są przetwarzane. Rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Zgoda osoby, której dane dotyczą - oznacza 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 Straży Miejskiej w Ziębicach, którą kieruje Komendant Straży Miejskiej w Ziębicach.
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 Komendant Straży Miejskiej w Ziębicach.
2. Osoba wyznaczona przez Komendanta Straży Miejskiej w Ziębicach 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

Komendant Straży Miejskiej w Ziębicach zapewnia zgodność przetwarzania danych osobowych z regulacjami DODO oraz krajowymi przepisami dotyczącymi ochrony danych osobowych -

szczególnie w odniesieniu do: pracowników i klientów Straży Miejskiej 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 stale podejmując działania w tym zakresie.
3. Prawa osób – Administrator umożliwia osobom, których dane przetwarza, wykonywanie i realizowanie ich praw.
4. Rozliczalność – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

2.2 Zasady ochrony danych

1. Komendant Straży Miejskiej w Ziębicach wypełnia obowiązki prawne, w szczególności wynikające z ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (t.j. Dz. U. z 2019 r. poz. 1795):
   1) w oparciu o podstawę prawną i zgodnie z prawem;
   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. 22-25 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) wraz ze wskazaniem ich praw (prawo uzyskania informacji o przetwarzaniu, prawo dostępu do danych, prawo do uzupełnienia, uaktualnienia lub sprostowania danych, prawo usunięcia danych)

3. Komendant Straży Miejskiej w Ziębicach na podstawie art. 34 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) zawiera umowy powierzenia z podmiotami przetwarzającymi. W tym celu prowadzi 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). Administrator powinien identyfikować przypadki przetwarzania wrażliwych danych osobowych. W tym przypadku Administrator postępuje zgodnie z zapisami art. 14 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).
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.
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 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 przez DODO oraz Ustawę o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości 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 (privacy 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) 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. Szacowanie ryzyka i ocena skutków.

Administrator tworzy ocenę ryzyka uwzględniającą charakter, zakres, kontekst i cele przetwarzania. Jeśli dany proces przetwarzania może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób Administrator tworzy ocenę skutków, określoną w art. 37 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

Ocena skutków to procedura, która jest tworzona w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń, głównie wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Ocena ryzyka oraz ocena skutków jest stworzona na potrzeby wykazania rozliczalności spełnienia wymagań DODO.

3.1 Szacowanie ryzyka

Ocena ryzyka (analiza ryzyka) jest to proces dążący do poznania charakteru oraz określenia poziomu ryzyka. W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z DODO oraz Ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Administrator powinien oszacować ryzyko właściwe dla przetwarzanych danych. Jeżeli wyniki szacowania ryzyka nie są zadowalające Administrator powinien wdrożyć środki, które powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufności, oraz uwzględnić stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie.

Analiza ryzyka jest przeprowadzana dla wszystkich istotnych kategorii osób zawartych w Rejestrze Czynności Przetwarzania.

Oceniając ryzyko Administrator powinien wziąć pod uwagę zagrożenia, które związane są z przetwarzaniem danych:

- przypadkowe lub niezgodne z prawem, zniszczenie, utracenie, zmodyfikowanie;

- nieuprawnione ujawnienie;

- nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

- pozostałe zagrożenia, które wynikają z listy zagrożeń, które prowadzi Administrator.

Jeżeli poziom ryzyka jest niezadowalający dla Administratora powinien on utworzyć Ocenę skutków.

3.2 Ocena skutków

Gdy operacje przetwarzania danych mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator powinien dokonać oceny skutków dla ochrony danych osobowych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka.

Wyniki oceny, należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z DODO oraz Ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania danych powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem tych danych Administrator powinien skonsultować się z organem nadzorczym.

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
Rzadkie – wystąpienie zagrożenia jest wysoce nieprawdopodobne w odniesieniu do analizowanej czynności lub charakter zagrożenia jest nieadekwatny do specyfiki czynności.	1
Mało prawdopodobne – zagrożenie występuje rzadziej niż co dziesięć lat lub brak jest informacji by zagrożenie występowało w podobnych podmiotach.	2
Możliwe – zagrożenie występuje co kilka lat lub zagrożenie wystąpiło w podobnych podmiotach w pojedynczych przypadkach.	3
Prawdopodobne – zagrożenie może wystąpić kilka razy w roku.	4
Prawie pewne – zagrożenie wystąpiło wielokrotnie w ciągu roku w danym podmiocie lub w podobnych podmiotach.	5

TABELA B - SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA
Bardzo niska – osoba, której dane dotyczą albo nie odczuje lub zetknie się z niewielką liczbą niedogodności, które bez problemu może przezwyciężyć	1
Niska – osoba, której dane dotyczą może napotkać znaczące niedogodności, które będzie w stanie przezwyciężyć, pomimo pewnych trudności.	2
Średnia – osoby, których dane dotyczą mogą napotkać znaczące konsekwencje, które powinny móc przezwyciężyć pomimo poważnych trudności.	3
Wysoka – osoby, których dane dotyczą mogą napotkać znaczące, a nawet nieodwracalne konsekwencje, których nie mogą przezwyciężyć.	4
Bardzo wysoka – osoby, których dane dotyczą mogą napotkać znaczące a nawet nieodwracalne konsekwencje w zakresie dóbr osobistych.	5

Załącznik Nr 1

			Skutek				
			Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
			1	2	3	4	5
Prawdopodobieństwo	Prawie pewne	5	Ś	W	K	K	K
	Prawdopodobne	4	Ś	W	W	K	K
	Możliwe	3	N	Ś	W	W	K
	Mało prawdopodobne	2	N	Ś	Ś	W	W
	Rzadkie	1	N	N	Ś	W	W

POZIOM RYZYKA	WARTOŚĆ
Niski (N)	Poziom ryzyka akceptowalny – działania podejmowane w zależności od wymaganych nakładów. Naruszenie bezpieczeństwa aktywa w zakresie Poufności, Integralności, Dostępności może w niewielkim stopniu utrudnić pracę z aktywem. Główne zadania w zakresie danego aktywa mogą być nadal realizowane. Brak znaczącego wpływu na wymagany poziom bezpieczeństwa informacji. Osoby, których dane osobowe są objęte zdarzeniem, praktycznie nie odczują skutków.
Średni (Ś)	Poziom ryzyka nieakceptowalny – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania. Naruszenie bezpieczeństwa aktywa w zakresie Poufności, Integralności, Dostępności może utrudnić pracę z aktywem, jednak można przywrócić pracę łatwo dostępnymi środkami. Naruszenie ma ograniczony wpływ na wymagany poziom bezpieczeństwa. Występuje niewielka odpowiedzialność finansowa. Raczej nie występują kary pieniężne lub są stosunkowo niskie. Osoby, których dane są objęte zdarzeniem, mogą odczuwać konsekwencje, które są w stanie rozwiązać pomimo kilku trudności.
Wysoki (W)	Poziom ryzyka nieakceptowalny – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania. Naruszenie bezpieczeństwa aktywa w zakresie Poufności, Integralności, Dostępności lub Poufności może znacząco zakłócić pracę z aktywem. Naruszenie ma istotny wpływ na bezpieczeństwo informacji. Możliwa jest odpowiedzialność prawna. Występuje średnia odpowiedzialność finansowa, w tym mogą

	występować średnie kary pieniężne. Występuje negatywny rozgłos medialny na skalę lokalną. Osoby, których dane osobowe są objęte zdarzeniem, mogą odczuwać istotne konsekwencje, które są w stanie rozwiązać z wieloma trudnościami.
Krytyczny (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania. Naruszenie bezpieczeństwa aktywa w zakresie Poufności, Integralności, Dostępności, drastycznie zakłóca lub całkowicie uniemożliwia pracę z aktywem. Naruszenie ma krytyczny wpływ na wymagany poziom bezpieczeństwa informacji. Występuje poważna odpowiedzialność prawna. Występuje poważna odpowiedzialność finansowa, w tym mogą występować wysokie kary pieniężne. Występuje negatywny rozgłos medialny na skalę krajową. Osoby, których dane osobowe są objęte zdarzeniem, mogą odczuwać istotne lub nawet nieodwracalne konsekwencje.

3.3.1. Reakcja na wartość ryzyka

1. Działania, które może zastosować Administrator wobec ryzyka:
    a. Modyfikowanie (redukcja) ryzyka – polega na zredukowaniu poziomu ryzyka przez taki wybór zabezpieczeń, aby ryzyko szczątkowe można było ponownie oszacować jak ryzyko akceptowalne.
    b. Zachowanie (akceptacja) ryzyka – polega na podjęciu decyzji o zachowaniu ryzyka bez podejmowania dalszych działań, na podstawie oceny ryzyka.
    c. Unikanie ryzyka – polega na unikaniu działań lub warunków, które powodują powstanie określonych ryzyk.
    d. Dzielenie (przeniesienie) ryzyka – na podstawie oceny ryzyka zaleca się transfer ryzyka do innej strony, która może skutecznie zarządzać ryzykiem
2. Analizę ryzyka przeprowadza się w specjalnym szablonie.

3.4 Plan postępowania z ryzykiem

1. Administrator prowadzi listę zabezpieczeń, których celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem.

2. Administrator prowadzi listę potencjalnych zagrożeń, które mogą spowodować niekorzystne skutki dla ochrony danych osobowych.
3. Administrator prowadzi listę podatności czyli słabości, które mogą być wykorzystane przez zagrożenia, powodując niekorzystne skutki dla ochrony danych osobowych.
4. 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.

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 systemami informatycznymi, w których zabezpieczenia są opisane w formie procedur.
2. Dokumenty powinny być aktualizowane, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka bądź 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 DODO oraz Ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości
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 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.

Załącznik Nr 1

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 zobowiązani są do zgłaszania IOD przypadków przetwarzania danych, ustania przyczyny przetwarzania uzasadniających wprowadzenie zmiany do RCPD, dążąc do tego aby wykazane były aktualne przypadki przetwarzania danych 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 przetwarzania,

   (b) wydział/ stanowisko osoby odpowiedzialnej za przetwarzanie danych,

   (c) opis kategorii osób,

   (d) opis kategorii danych osobowych,

   (e) w jakiej formie są przetwarzane dane osobowe (dokumenty papierowe/ oprogramowanie)

   (f) opis kategorii odbiorców danych

   (g) źródło danych

   (h) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu,

   (i) cel przetwarzania danych

   (j) planowany termin usunięcia danych osobowych

(k) informację o przekazaniu danych poza UE

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 Straży Miejskiej 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. Strażnik Miejski 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 3 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie

swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.).

2. IOD w wykonywaniu swoich zadań podlega bezpośrednio Komendantowi Straży Miejskiej w Ziębicach.

3. Do zadań IOD należy w szczególności:

1) informowanie Komendanta Straży Miejskiej w Ziębicach oraz Strażników Miejskich, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia DODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach;

2) monitorowanie przestrzegania dyrektywy 2016/680 z dnia 27 kwietnia 2016 r., 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. 27 DODO;

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 DODO 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

1. Zgodnie z art. 29 DODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
2. Administrator dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem informacji. Dla poszczególnych obszarów i systemów krytycznych tworzone są plany postępowania w sytuacjach awaryjnych i kryzysowych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności organizacji oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami.
3. O konieczności tworzenia planu ciągłości działania dla konkretnego z systemu decyduje Administrator.
4. Administrator zgodnie z planem postępowania w procesie analizy ryzyka i szacowania skutków przekazuje w formie elektronicznej bądź pisemnej treść zaleceń do osób odpowiedzialnych za ich wdrożenie z jednoczesnym uwzględnieniem terminu realizacji.

Załącznik Nr 2

Regulamin Ochrony Danych Osobowych W Straży Miejskiej w Ziębicach

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

Spis treści:

1 Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów....3

2 Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy....3

3 Zabezpieczenie dokumentacji papierowej z danymi osobowymi....4

4 Polityka haseł....4

5 Zasady wynoszenia nośników z danymi poza miejsce pracy....5

6 Zasady korzystania z Internetu....6

7 Zasady korzystania z poczty elektronicznej....6

8 Ochrona antywirusowa....7

9 Zasady zabezpieczania kluczy....8

10 Obowiązek zachowania poufności i ochrony danych osobowych....8

11 Zasady współpracy z IOD....9

12 Postępowanie dyscyplinarne....9

Załącznik Nr 2

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 Administratorowi Systemu Informatycznego 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. Użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienia stanowiące załącznik nr 1, ponadto każdy użytkownik zobowiązany jest do podpisania oświadczeń o zachowaniu poufności przetwarzanych danych osobowych stanowiących załącznik nr 2.
2. 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.
3. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na wniosek przełożonego a wykonywane jest przez Administratora Systemu Informatycznego.
4. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).
5. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
6. Zabrania się pracy wielu użytkowników na wspólnym koncie.

7. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
8. Użytkownik jest zobowiązany do powiadomienia Administratora Systemu Informatycznego o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
9. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym Administratora Systemu Informatycznego.
10. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach – tzw. polityka czystego ekranu.
11. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
12. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako Administrator Systemu Informatycznego . Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
13. 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 Straży Miejskiej 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 Straży Miejskiej 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 budynku Straży Miejskiej 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 budynku Straży Miejskiej 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 Administratora Systemu Informatycznego 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, 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 przekierowania do stron z „wirusami". Użytkownik otwierając taki hiperlink infekuje komputer oraz inne komputery w sieci. Po ich otwarciu istnieje wysokie ryzyko bezpowrotnej utraty danych.
8. Należy zgłaszać Administratorowi Systemu Informatycznego 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 Administratora Systemu Informatycznego lub osobę upoważnioną.

9 Zasady zabezpieczania kluczy

1. Administrator danych 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 Komendanta Straży Miejskiej w Ziębicach. 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 Straży Miejskiej w Ziębicach, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.
6. Obowiązek zachowania w tajemnicy danych osobowych, które pracownik pozyskał w trakcie zatrudnienia w Straży Miejskiej 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 Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.) oraz Ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

Załącznik nr 1 do Regulaminu Ochrony
Danych Osobowych w Straży Miejskiej
w Ziębicach

Ziębice, dn. ..... 20..... r.

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 23 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW – (dyrektywa policyjna). – dalej **DODO** – nadaję upoważnienie Pani/Panu:

.....

(imię i nazwisko)

.....

(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku. Uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych w zakresie określonym przez Komendanta Straży Miejskiej w Ziębicach.

Jednocześnie upoważniam Panią/Pana do przetwarzania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, w ramach wyznaczonego zakresu obowiązków oraz pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Straży Miejskiej w Ziębicach.

Równocześnie zobowiązuję Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami DODO, prawem polskim, a także z polityką bezpieczeństwa informacji pracodawcy.

.....

podpis osoby uprawnionej
do nadania upoważnienia

Załącznik nr 2 do Regulaminu Ochrony
Danych Osobowych w Straży Miejskiej
w Ziębicach

..... Ziębice, dn. ..... 20..... r..

(Imię, Nazwisko,Stanowisko)

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznałam/em się z przepisami w zakresie ochrony danych osobowych obowiązującymi w Straży Miejskiej w Ziębicach, w szczególności z przepisami Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WsiSW, ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz Polityką Ochrony Danych Osobowych obowiązującą w Straży Miejskiej w Ziębicach.

Zobowiązuję się do:

* przetwarzania danych osobowych wyłącznie w zakresie i celu niezbędnym do realizacji powierzonych przez Pracodawcę obowiązków,
* zachowania poufności danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem obowiązków powierzonych przez Pracodawcę,
* niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych obowiązków przez Pracodawcę,
* zachowania poufności dotyczącej sposobów zabezpieczenia danych osobowych,
* ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Pracodawcę za naruszenie przepisów o ochronie danych osobowych oraz będzie traktowane jako naruszenie podstawowych obowiązków pracowniczych.

.....

(podpis oświadczającego)

Załącznik Nr 3

Instrukcja zarządzania systemami informatycznymi w Straży Miejskiej w Ziębicach

Załącznik Nr 3

1. Wstęp....3
2. Zabezpieczenia fizyczne....3
3. Procedura nadawania uprawnień do przetwarzania danych osobowych....3
4. Metody i środki uwierzytelnienia (polityka haseł)....4
5. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych....5
6. Procedura zabezpieczenia systemu informatycznego....5
   6.1. Bezpieczeństwo przetwarzania danych poza Strażą Miejską w Ziębicach....5
   6.2. Zabezpieczenia infrastruktury IT....6
   6.3. Zabezpieczenia aplikacji....6
7. Procedura wykonywania przeglądów i konserwacji....6

Załącznik Nr 3

1. Wstęp

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 39 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), 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.
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. Złącze główne zabezpieczono w szafach zamykanych na klucz.
6. Dostęp do pomieszczeń biurowych zabezpieczono drzwiami antywłamaniowymi oraz zamykanymi na klucz.
7. Dokumentację zabezpieczono w zamkniętych na klucz niemetalowych szafach. Dokumentację pracowniczą zabezpieczono w zamkniętych na kod metalowych szafach.
8. Pomieszczenia chronione są przez system alarmowy oraz kraty.
9. Stosowana jest Polityka kluczy.

3. 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 Administrator Systemu Informatycznego.

5. Powyższą procedurę wykonuje się poprzez przesłanie wniosku według załącznika o nadanie/modyfikację/odebranie zakresu uprawnień w systemie informatycznym e-maila przez Komendanta Straży Miejskiej w Ziębicach do Administratora Systemu Informatycznego z prośbą o dostęp do odpowiedniego wydziałowego katalogu. W tym przypadku stosuje się załączony wniosek o dostęp do uprawnień.
6. W przypadku zmiany stanowiska pracy lub zakresu czynności, przełożony osoby upoważnionej do przetwarzania danych składają wniosek według załącznika o nadanie/modyfikację/odebranie zakresu uprawnień w systemie informatycznym.
7. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
8. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.
9. 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.
10. Stosowany jest system uwierzytelniania Windowsa z wykorzystaniem loginu i hasła.

4. 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 Administratora Systemu Informatycznego osobie zastępującej administratora
8. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

5. 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 budynku Straży Miejskiej 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.

6. Procedura zabezpieczenia systemu informatycznego

6.1. Bezpieczeństwo przetwarzania danych poza Strażą Miejską w Ziębicach

1. Użytkownicy komputerów przenośnych wynoszonych poza obszar Straży Miejskiej 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 Straży Miejskiej w Ziębicach.
3. Dane osobowe na komputerach przenośnych wynoszonych poza obszar Straży Miejskiej w Ziębicach muszą być przechowywane na zaszyfrowanych partycjach.
4. Dyski przenośne oraz pendrive wynoszone poza budynek Straży Miejskiej 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 Administratora Systemu Informatycznego.
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.

6.2. Zabezpieczenia infrastruktury IT

1. Zastosowano blokadę portów USB, DVD, CD na stacjach roboczych.
2. Zabezpieczono hasłem dostęp do portów fizycznych gniazd szeregowych, USB, Ethernet celem uniemożliwienia zmian konfiguracji przez osoby nieupoważnione.
3. Dokonano dezaktywacji nieużywanych gniazd sieciowych przez wypięcie przewodów lub wyłączenie portów na switchu.
4. Drukarki z funkcją kontroli wydruków.
5. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu", aktywowane po 3 minutach nieaktywności użytkownika
6. Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne

6.3. 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.

7. Procedura wykonywania przeglądów i konserwacji

1. Stosowany jest system do monitoringu aktywności użytkowników.
2. Administratora Systemu Informatycznego jest odpowiedzialny za monitoring, przegląd logów aktywności aplikacji, baz oraz uprawnień użytkowników i administratorów.

3. Administrator Systemu Informatycznego odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków, optymalizację baz danych.
4. Administrator Systemu Informatycznego odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email.
5. Administrator Systemu Informatycznego odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
6. 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.
7. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z jednostek zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
8. 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 Nr 1 do Instrukcji zarządzania RODO
w Straży Miejskiej w Ziębicach

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 Straży Miejskiej	
Inne:	

Programy:	
FK 2000	
Finn	
Lex	
Bip	
Strona internetowa	
E-mail	
Podpis elektroniczny	
Inne	

Uwagi:

Data i podpis bezpośredniego przełożonego:	
Data i podpis Informatyka:	Data i podpis IOD:

Załącznik Nr 2 do Instrukcji zarządzania RODO
w Straży Miejskiej 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

Procedura postępowania z incydentami

Spis treści

1. Wstęp.....2

2. Postępowanie w przypadku naruszenia danych osobowych.....2

3. Naruszenie danych osobowych– odpowiedzialność.....4

4. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu.....4

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

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 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. Administrator Systemu Informatycznego 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 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.

Załącznik Nr 4

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 dostęp osobom nieuprawnionym 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 5

Procedura realizacji praw osób, których dane dotyczą

Spis treści

1 Wstęp....2

2 Odnotowywanie zgłoszeń....2

3 Schemat załatwienia sprawy....3

4 Informacje o prawie do wniesienia skargi do organu nadzorczego....5

5 Współpraca z innymi podmiotami....5

6 Tryb Odwoławczy....6

7 Dodatkowe informacje....6

8 Prawo dostępu do danych....6

9 Prawo sprostowania danych....7

10 Prawo do usunięcia danych....7

11 Prawo do ograniczenia przetwarzania....8

1 Wstęp

1. Administrator danych weryfikuje i zapewnia możliwość efektywnego wykonania praw podmiotu, zapewniając jednocześnie odpowiednie warunki, aby prawa podmiotu były realizowane niezwłocznie, w sposób wymagany przez Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.). oraz Ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

2. Osobie, której dane dotyczą przysługują prawa na mocy art. 22-25 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125). :
- prawo dostępu do swoich danych,
- prawo do uzupełnienie, uaktualnienie lub sprostowanie danych osobowych - w przypadku gdy dane te są niekompletne, nieaktualne lub nieprawdziwe;
- prawo do usunięcia danych osobowych - w przypadku gdy dane te zostały zebrane lub są przetwarzane z naruszeniem przepisów,
- prawo ograniczenia przetwarzania danych.

ADO podejmuje odpowiednie środki aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie której dane dotyczą wszelkich informacji dotyczących realizacji jej praw.

3. Ze względu na wykonywanie zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Komendantowi Straży Miejskiej jako Administratorowi niektóre prawa osoby, o których mowa w art. 22-25 mogą nie mieć zastosowania lub mogą być ograniczone na podstawie Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) lub przepisów szczególnych.

4. Administrator Danych ułatwia podmiotowi danych realizację jego praw wskazanych w art. 22-25 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125). Przyjmuje się następujące sposoby przekazywania informacji służące ułatwianiu zgłaszania żądań:
Adres mailowy: straz_miejska@ziebice.pl , iod@ziebice.pl
Osobiście lub listownie na adres siedziby Administratora: Komendant Straży Miejskiej w Ziębicach, Plac Strażacki nr 8, 57-220 Ziębice.

2 Odnotowywanie zgłoszeń

1. W ramach zgłoszonych żądań i odpowiedzi Komendant Straży Miejskiej w Ziębicach (lub upoważniony pracownik) będzie odnotowywać m.in. wpływ żądania (kto, kiedy, jakiej treści i w jaki sposób) i udzielenia odpowiedzi na żądanie (kto, kiedy, jakiej treści, w jaki sposób) a także sposób spełnienia obowiązku wskazując przy tym termin realizacji prawa podmiotu. Rejestr realizacji praw stanowi załącznik nr 2.

2. Każdy pracownik do którego trafia żądanie w ramach prawa podmiotu jest zobowiązany do niezwłocznego poinformowania o tym Komendanta Straży Miejskiej w Ziębicach (lub upoważnionego pracownika) i przekazania mu treści żądania. Komendant Straży Miejskiej w Ziębicach (lub upoważniony pracownik) ocenia komunikat pod kątem zgodności z przepisami Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).
Inspektor Ochrony Danych jest punktem kontaktowym dla osób, których dane dotyczą. Osoby te, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw.

3. IOD nie może być odpowiedzialny za podejmowanie decyzji co do tego czy żądanie uwzględnić i w jaki sposób. W tym zakresie Administrator Danych powinien konsultować się z IOD.

4. Komendant Straży Miejskiej w Ziębicach ostatecznie decyduje o tym czy pozytywnie zrealizować żądanie. Osoba technicznie realizująca wniosek odpowiada wyłącznie za techniczny aspekt realizacji praw (działa na polecenie właściciela procesu).
5. Upoważniony pracownik lub IOD:
   a) kieruje żądanie do właściciela procesu w celu podjęcia decyzji co do sposobu realizacji żądania;
   b) kieruje żądanie (w oparciu o decyzję właściciela procesu) do osoby wykonującej technicznie żądanie;
   c) prowadzi korespondencję z osobą żądającą (chyba, że prowadzi ją IOD);
   d) wypełnia ewidencję praw podmiotów.

3 Schemat załatwienia sprawy

1. Po otrzymaniu żądania upoważniony pracownik lub IOD (przy współpracy z właścicielem procesu) rejestruje żądanie w ewidencji praw podmiotów:
   a) weryfikuje rodzaj żądania i w razie wątpliwości prosi osobę, żądającą o podanie dodatkowych informacji umożliwiających sprecyzowanie żądania;
   b) ustala w ramach jakiej kategorii podmiotów należy identyfikować zgłaszającego;

c) na podstawie wykazu czynności przetwarzania określa się jaki zakres danych jest istotny z punktu widzenia identyfikacji danych osoby zgłaszającej żądanie (odszukania tych danych i przypisania do wyodrębnionej osoby) oraz weryfikacji tożsamości osoby żądającej Np. jeżeli określoną osobę identyfikujemy poprzez adres e-mail proszenie o PESEL celem weryfikacji tożsamości stanowić będzie przetwarzanie danych nadmiarowych. Dana osoba fizyczna może być identyfikowana w ramach różnych procesów poprzez inny zestaw danych osobowych .

W ramach powyższych czynności należy konsultować się z IOD.

2. Jeżeli Administrator będzie mógł wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. W takim przypadku osoba, której dane dotyczą, w celu wykonania praw jej przysługujących będzie musiała dostarczyć dodatkowe informacje pozwalające ją zidentyfikować. Dodatkowo, Administrator może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą, jeśli będzie miał uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie.

3. Niedopuszczalne jest przekazywanie informacji zwrotnej przed zweryfikowaniem tożsamości. Prosząc o dodatkowe dane np. w celu sprecyzowania żądania, w celu identyfikacji lub weryfikacji tożsamości należy wyraźnie poinformować osobę żądającą o celu pozyskania tych dodatkowych informacji (można również wyznaczyć dodatkowy termin na ich przekazanie) oraz wskazać, że bez tych informacji realizacja praw w całości lub w części nie będzie możliwa. Weryfikacja tożsamości nie może prowadzić do gromadzenia danych w sposób nadmierny i musi być adekwatna do poziomu ryzyka. W toku realizacji praw podmiotów danych odpowiednie może okazać się zaczerpnięcie opinii IOD.

Należy zawsze weryfikować podstawę umocowania, gdy osoba żądająca wskazuje, że działa w imieniu innego podmiotu.

4. W następnej kolejności należy:

a) sprawdzić, czy żądanie jest możliwe do zrealizowania oraz czy nie zachodzą przesłanki wyłączające możliwość realizacji żądania, ewentualnie przesłanki pobrania opłaty;
b) zweryfikować czas oraz środki potrzebne na realizację żądania, a także kto będzie odpowiedzialny za techniczną obsługę żądania oraz podjęcia decyzji o sposobie realizacji żądania;
c) jeżeli żądanie jest zasadne należy przekazać odpowiedź podmiotowi, który wniósł żądanie, wskazując sposób oraz termin realizacji żądania;
d) odnotować sposób realizacji żądania ewidencji praw podmiotów.

5. Należy uwzględnić, iż informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Dotyczy to zarówno budowy standardowego komunikatu jak i w ramach realizacji zindywidualizowanych żądań. Ustne przekazywanie informacji należy uznać za wyjątek (jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami

potwierdzi się tożsamość osoby, której dane dotyczą). Ustne udzielenie informacji powinno zostać odnotowane w celu zapewnienia rozliczalności.

6. Odpowiadając na żądanie należy uwzględnić sposób zgłoszenia żądania. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

7. Realizacja praw jest co do zasady wolna od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:
- pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań;
- odmówić podjęcia działań w związku z żądaniem.
Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

8. Wniosek dotyczący praw osoby, której dane dotyczą co do zasady realizowany jest niezwłocznie i zależy od stopnia skomplikowania jak również jest zróżnicowany w zależności od kategorii obowiązków wobec niego.

4 Informacje o prawie do wniesienia skargi do organu nadzorczego

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 Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.).
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. 50 DODO.
Każda osoba fizyczna ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna iż przetwarzanie danych osobowych jej dotyczących narusza przepisy DODO.

W celu skorzystania z przysługujących praw osoba której dane dotyczą powinna dostarczyć do Administratora wniosek:

Osobiście / pisemnie: Komendant Straży Miejskiej w Ziębicach, Plac Strażacki 8, 57-220 Ziębice

Elektronicznie: e-mail na adres: iod@ziebice.pl

Za pośrednictwem ePuap przy wykorzystaniu np. wzoru „pismo ogólne do podmiotu publicznego"

5 Współpraca z innymi podmiotami.

1. W przypadku powierzenia danych przez Administratora procesor powinien wspomóc Administratora Danych w realizacji praw podmiotu. Służyć temu ma weryfikacja procesora zgodnie z art. 34 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

2. Gdyby dochodziło do współadministrowania danymi, kwestię realizacji praw podmiotu uzgadnia się z pozostałymi współadministratorami ustalając odpowiednie zakresy swojej odpowiedzialności, chyba że przypadające im obowiązki i ich zakres określa prawo UE lub prawo państwa członkowskiego. Wskazane uzgodnienia muszą odzwierciedlać zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

6 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 na adres ul. Stawki 2 00-193 Warszawa oraz skorzystania ze środków ochrony prawnej przed sądem.

7 Dodatkowe informacje

1. Żądania podmiotów danych są rozpoznawane w sposób najbardziej korzystny dla podmiotów danych, a w razie uzasadnionych wątpliwości uzyskiwane są dodatkowe informacje.

2. Podstawa prawna:

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.). zwanym wyżej "rozporządzeniem 2016/680", DODO.

Załącznik nr 5

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

8 Prawo dostępu do danych.

1. Prawo dostępu do danych obejmuje możliwość:
   - uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące;
   - uzyskania katalogu informacji zgodnych z art. 23 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

2. Podmiot danych ma także prawo do uzyskania kopii danych.

3.Prawo dostępu do danych obejmuje wszystkie dane które dotyczą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, łącznie z danymi zaobserwowanymi i wywnioskowanymi na jej temat.

4. Należy weryfikować zawsze czy prawo do uzyskania kopii może niekorzystnie wpływać na prawa i wolności innych osób, w tym własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji.

5. Jeżeli Administrator Danych będzie przetwarzać duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje
lub czynności przetwarzania, których dotyczy jej żądanie.

6. Jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny.

7. Należy pamiętać, że osoba, której dane dotyczą, może żądać realizacji wszystkich przysługujących jej praw także w odniesieniu do danych zarchiwizowanych już przez administratora. Mogą być one realizowane przez podmiot danych zarówno osobiście, jak i przez jego przedstawiciela ustawowego czy pełnomocnika.

9 Prawo sprostowania danych.

1. Dopuszcza się dwie formy sprostowania danych: sprostowanie rozumiane jako poprawienie nieprawidłowych danych oraz sprostowanie rozumiane jako uzupełnienie niekompletnych danych, a więc przedstawienie dodatkowych informacji.

2. Uzupełnienie danych nie może obejmować danych, które byłyby nadmierne, tj. takich, które nie spełniałyby wskazanej wyżej przesłanki niezbędności – stanowiłoby to naruszenie zasady minimalizacji danych. Przedmiotem uzupełnienia nie mogą być też dane, które są nieprawidłowe.

3. Administrator Danych ma obowiązek poinformować o sprostowaniu danych osobowych, którego dokonał w ramach żądania podmiotu danych, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. „Ujawnienia" danych rozumiane są szeroko, jako jakiekolwiek możliwości zapoznania się z danymi osobowymi. Administrator Danych ma obowiązek informować osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

10 Prawo do usunięcia danych

1. Żądanie usunięcia danych należy wnikliwie analizować pod kątem aktualności przesłanek wyłączających możliwość usunięcia danych. Administrator Danych nie ma obowiązku usuwać danych jeżeli jest to niezbędne:
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa UE lub prawa państwa członkowskiego, któremu podlega administrator;
- do ustalenia, dochodzenia lub obrony roszczeń.

2. Analizując podstawy odmowy żądania usunięcia danych należy odwołać się do rejestru czynności i opisanych w nim celów przetwarzania danych.

3. Należy określić techniczną możliwość usunięcia danych w razie uzasadnionego żądania usunięcia danych osobowych. Dotyczy to zarówno pojedynczych danych jak i całych zbiorów.

4. Należy zidentyfikować powiązania pomiędzy bazami danych, które mogą uniemożliwić usuwanie danych osobowych. Samo rozproszenie danych pomiędzy różnymi bazami czy systemami nie wyklucza możliwości żądania usunięcia wszystkich danych.

5. Jeżeli Administrator Danych upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – obowiązany jest podjąć rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

6. Jeżeli usunięcie danych może utrudnić realizację innych praw to należy o tym poinformować podmioty żądające usunięcia.

11 Prawo do ograniczenia przetwarzania.

1. Należy przesądzić w jaki techniczny sposób realizowane będzie prawo do ograniczenia przetwarzania.

2. Wśród metod pozwalających ograniczyć przetwarzanie danych osobowych znajdują się między innymi:
- czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania,
- uniemożliwienie użytkownikom dostępu do wybranych danych,
- czasowe usunięcie opublikowanych danych ze strony internetowej.

3. Fakt ograniczenia przetwarzania danych osobowych należy wyraźnie zaznaczyć w systemie (jeżeli dane osobowe są przetwarzane w systemie).

4. Przed uchyleniem ograniczenia przetwarzania informuje się o tym osobę, której dane dotyczą, która żądała ograniczenia przetwarzania.

5. Administrator Danych informuje o ograniczeniu przetwarzania danych osobowych, którego dokonał w ramach zgłoszonego żądania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. „Ujawnienia" danych należy rozumieć szeroko, jako jakąkolwiek możliwość zapoznania się z danymi osobowymi.

6. Jeżeli osoba, której dane dotyczą, tego zażąda, Administrator informuje osobę, której dane dotyczą, o tych odbiorcach.

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

.....
(miejscowość, data)

Wniosek osoby, której dane dotyczą

Komendant Straży Miejskiej
w Ziębicach
Plac Strażacki 8
57-220 Ziębice

Imię i nazwisko wnioskodawcy	
Adres korespondencyjny	
PESEL	
Dane kontaktowe (Tel. e-mail)	
Zakres żądania:	a prawo do informacji i kopii danych b prawo do sprostowania danych c prawo do usunięcia danych d prawo do ograniczenia przetwarzania
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 2 do Procedury realizacji praw osób, których dane dotyczą

Rejestr realizacji praw osób

Lp.	Naruszenie (stypizowany opis naruszenia)	Data i godzina zgłoszenia podejrzenia naruszenia	Data oraz godzina stwierdzenia naruszenia	Data naruszenia/okres, którego dotyczy	Kategoria i ilość osób, których dotyczy naruszenie	Zakres danych i/lub kategorie danych, których dotyczy naruszenie	Osoba/źródło informacji o zdarzeniu	Miejsce naruszenia	Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia

Opis skutków/konsekwencji naruszenia	Osoba/jednostka odpowiedzialna za naruszenie	Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki zastosowane w celu zminimalizowania jego negatywnych skutków	Rezultat działań naprawczych	Osoba odpowiedzialna za wdrożenie działań naprawczych	Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych (Jeśli tak - data i godzina zgłoszenia; w przypadku wystąpienia opóźnienia w powiadomieniu - wyjaśnienie przyczyn opóźnienia)	Czy poinformowano organy ścigania (data zawiadomienia)	Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy oraz sposób przekazania informacji wraz opisem zaleceń dla podmiotów danych	Monitoring działań naprawczych

Załącznik nr 6

POLITYKA CZYSTEGO BIURKA I EKRANU W STRAŻY MIEJSKIEJ W ZIĘBICACH

1. Niniejsza Polityka Czystego Biurka obowiązuje wszystkich pracowników zatrudnionych w Straży Miejskiej w Ziębicach.

2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, a także każdą osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, praktykanta, stażystę oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.

3. Pracodawcą jest Urząd Miejski w Ziębicach, z siedzibą przy ul. Przemysłowa 10, 57-220 Ziębice, którego kierownikiem jest Burmistrz Ziębic.

4. Pomieszczenia w których realizowane są czynności przetwarzania danych chronionych muszą być zamykane na klucz. Miejsca (np. szafy, szuflady w biurku itp.) przeznaczone do przechowywania danych chronionych także muszą być zamykane na klucz. Miejsca te mogą być otwarte tylko na czas niezbędny do wykonania bieżących zadań, a następnie zostają zamknięte.

5. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do realizacji bieżących zadań.

6. Każdy komputer musi mieć aktywny wygaszasz ekranu z dostępem do danych po podaniu hasła, wyłączający się automatycznie po określonym czasie bezczynności użytkownika. Dodatkowo przed pozostawieniem włączonego komputera bez nadzoru użytkownik jest zobowiązany wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.

7. Po zakończonej pracy pracownik zobowiązany jest umieścić wszystkie dokumenty zawierające dane chronione w zamykanych na klucz szafach i biurkach. Klucze do tych miejsc pozostają w wyłącznej dyspozycji pracownika Straży Miejskiej w Ziębicach. Po zakończonej pracy pracownik zobowiązany jest wyłączyć komputer oraz monitor.

8. Niedopuszczalne jest pozostawianie otwartego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu, jeśli nie pozostaje w nim osoba uprawniona. Po zakończeniu dnia pracy, ostatni pracownik opuszczający pomieszczenie jest zobowiązany zamknąć wszystkie okna i drzwi oraz zgodnie z obowiązującymi ustaleniami, zabezpieczyć klucze do pomieszczenia.

9. Po zakończonej pracy pracownik zobowiązany jest umieścić laptopa w zamykanej na klucz szafie.

10. W sytuacjach nagłych, związanych w szczególności ze stanem zdrowia pracownika lub sytuacją polegającą na przedłużającej się nieobecności na stanowisku pracy, za realizację postanowień niniejszego dokumentu w jego imieniu odpowiadają solidarnie pracownicy, przebywający w tym samym pomieszczeniu służbowym.

11. Wydruki robocze zawierające informacje chronione, błędne lub zdezaktualizowane muszą być niezwłocznie bezpowrotnie niszczone przy użyciu niszczarki do papieru lub w inny sposób, zapewniający skuteczne ich usunięcie lub anonimizowanie. Każdy użytkownik odpowiada za przetwarzane przez niego zasoby. Zasoby te przeznaczone są do realizacji celów służbowych. Wykorzystywanie ich w innym celu niż służbowy jest bezwzględnie zabronione.

Załącznik Nr 7

Polityka kluczy

1. Polityka kluczy obejmuje pomieszczenia Straży Miejskiej w Ziębicach przy Placu Strażackim 8, 57-220 Ziębice.
2. Obowiązuje pięciodniowy tydzień pracy, od poniedziałku do piątku, w godzinach 7:00-15:00
3. Dostęp do pobierania kluczy do biur Straży Miejskiej w Ziębicach mają wyłącznie osoby upoważnione przez Komendanta Straży Miejskiej w Ziębicach. Osoby upoważnione do posiadania kluczy to:
   a) Bartosz Kulin – starszy inspektor Straży Miejskiej
   b) Stanisław Sala – starszy inspektor Straży Miejskiej
   c) Mariusz Kopciński – starszy inspektor Straży Miejskiej
   d) Andrzej Tomczuk – starszy inspektor Straży Miejskiej
4. Dostęp do odblokowania alarmu do pomieszczeń szczególnie chronionych w budynku Straży Miejskiej w Ziębicach mają wyłącznie osoby upoważnione przez Komendanta Straży Miejskiej w Ziębicach.
5. 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.
6. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane (symbol wydziału oraz numer szafki).
7. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
8. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
9. Po zakończeniu pracy klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
10. 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.
11. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2020 r. poz. 1320 z późn. zm.). oraz z art. 363 § 1 Ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2020 r. poz. 1740 z późn. zm.).