Zarządzenie nr 31/2024

Dyrektora Zarządu Transportu Miejskiego w Kielcach
z dnia 31 grudnia 2024 r.

w sprawie wprowadzenia Polityki Ochrony Danych w Zarządzie Transportu Miejskiego w Kielcach w oparciu o przepisy ogólnego rozporządzenia o ochronie danych (RODO)

Na podstawie art. 24 ust. 1 i ust. 2 w związku z art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) oraz § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247), zarządzam, co następuje:

§ 1

Mając na uwadze konieczność wdrożenia odpowiednich środków technicznych i organizacyjnych, mających na celu zapewnienie spełnienia wymogów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „RODO", wprowadzam Politykę Ochrony Danych w Zarządzie Transportu Miejskiego w Kielcach, stanowiącą załącznik do niniejszego zarządzenia, zwaną dalej „Polityką".

§ 2

Opracowana na podstawie RODO Polityka stanowi podstawowy dokument zawierający zasady i wymagania ochrony posiadanych danych, ze szczególnym uwzględnieniem danych osobowych, a zwłaszcza przechowywanych i przetwarzanych w ramach systemów informatycznych.

§ 3

1. Każda osoba fizyczna uzyskująca dostęp do zasobów informacyjnych w Zarządzie Transportu Miejskiego w Kielcach musi zostać zapoznana z przepisami RODO oraz z Polityką i zobowiązać się do ich przestrzegania.
2. Obowiązek, o którym mowa w ust. 1, dotyczy przede wszystkim pracowników, stażystów, praktykantów, a także osób działających z upoważnienia podmiotu przetwarzającego dane osobowe.

§ 4

Nadzór nad wykonaniem niniejszego zarządzenia sprawuje Inspektor Ochrony Danych.

§ 5

Traci moc Zarządzenie Dyrektora Zarządu Transportu Miejskiego nr 4/2022 z dnia 01 marca 2022r.

§ 6

Zarządzenie wchodzi w życie z dniem 31 grudnia 2024 r.

ZATWIERDZAM

Otrzymują:

GK

EA

NT

NP.

ND

NO

Załącznik
do Zarządzenia nr 31/2024
Dyrektora Zarządu Transportu Miejskiego
w Kielcach
z dnia 30.12.2024 r.

POLITYKA OCHRONY DANYCH W ZARZĄDZIE TRANSPORTU MIEJSKIEGO W KIELCACH

Kielce 2024

Rozdział I
POSTANOWIENIA OGÓLNE

§ 1

Idea systemu ochrony danych

1. Dane - rozumiane jako wszelkie informacje, które mogą być przetwarzane, bez względu na ich formę - podobnie jak inne ważne aktywa, są niezbędne do funkcjonowania każdej jednostki i z tego powodu zaleca się ich odpowiednią ochronę.
2. Realizacja statutowych zadań jednostki wymaga, między innymi, efektywnego dostępu do danych oraz zapewnienia odpowiedniego poziomu bezpieczeństwa informacji.
3. Bezpieczeństwo informacji oznacza jej ochronę przed szerokim spektrum zagrożeń w celu zachowana poufności, integralności i dostępności informacji, a także minimalizacji ryzyka oraz zapewnienia ciągłości działania jednostki i realizacji jej zadań statutowych na odpowiednim poziomie. Utrata poufności, integralności, dostępności, autentyczności lub niezawodności może mieć negatywny wpływ na bieżącą działalność lub wizerunek jednostki.
4. Bezpieczeństwo danych można osiągnąć wdrażając odpowiednie środki techniczne i organizacyjne, którymi mogą być polityki, procesy, procedury, struktury organizacyjne, zabezpieczenia fizyczne oraz funkcje oprogramowania i sprzętu.
5. Środki, o których mowa w ust. 4, winny być w szczególności zgodne z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń.

§ 2

Cel Polityki Ochrony Danych

1. Polityka Ochrony Danych jest zbiorem zasad i procedur, którym muszą podporządkować się osoby posiadające dostęp do zasobów informacyjnych. Określa również zasady ochrony infrastruktury, zasobów informatycznych i ludzkich.
2. Celem Polityki Ochrony Danych jest taki opis struktury oraz sposobu funkcjonowania systemu bezpieczeństwa informacji funkcjonującego w Zarządzie Transportu Miejskiego w Kielcach, aby zapewnić właściwą ochronę zasobów informacyjnych jednostki.

§ 3

Słownik pojęć

Występujące w Polityce Ochrony Danych zwroty oznaczają:

1) **ZTM** – Zarząd Transportu Miejskiego w Kielcach, ul. Głowackiego 4, 25-368 Kielce,
2) **Polityka** – Polityka Ochrony Danych obowiązująca w ZTM,
3) **Dane osobowe** – to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba,

której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powoływanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe i społeczne,

4) **Dane szczególnej kategorii (dane wrażliwe, informacja wrażliwa**) **–** to taka informacja, której nieuprawnione upublicznienie (ujawnienie) może mieć szkodliwy wpływ na wykonywanie zadań oraz wizerunek ZTM i które winny być przechowywane w warunkach uniemożliwiających ich nieuprawnione ujawnienie i wykorzystanie. To dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, służące jednoznacznemu zidentyfikowaniu osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.
5) **Przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, a zwłaszcza te które wykonuje się w systemach informatycznych,
6) **Ograniczenie przetwarzania** – to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania,
7) **Profilowanie** – rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które 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,
8) **Pseudonimizacja (anonimizacja)** – rozumie się przez to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
9) **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
10) **Administrator Danych Osobowych (ADO)** – Dyrektor ZTM, decydujący o celach i środkach przetwarzania danych osobowych oraz wdrażający w tym celu odpowiednie środki techniczne i organizacyjne,
11) **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez ADO, będąca pracownikiem ZTM lub zatrudniona na podstawie umowy cywilnoprawnej, odpowiedzialna za nadzór nad przetwarzaniem danych osobowych, w tym m.in. za analizę zagrożeń, wdrażanie stosownych środków organizacyjnych, administracyjnych, technicznych i fizycznych w celu zabezpieczenia danych osobowych przed ich naruszeniem, zwany dalej „IOD". W przypadku nie powołania w ZTM Administratora Systemu Informatycznego (ASI), zakres odpowiedzialności IOD w ZTM może zostać przez ADO rozszerzony o zakres obowiązków ASI,

12) **Administrator Systemu Informatycznego (ASI)** – osoba wyznaczona przez ADO, będąca pracownikiem ZTM lub zatrudniona na podstawie umowy cywilnoprawnej, odpowiedzialna za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w systemie, realizująca zadania związane z eksploatacją systemu teleinformatycznego przetwarzającego dane osobowe, ze szczególnym uwzględnieniem dystrybucji haseł dostępu i uprawnieniami technicznymi osób do dostępu do systemu, a także odpowiedzialna za zabezpieczanie sieci komputerowej,
13) **Podmiot przetwarzający (procesor)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu ADO,
14) **Przedstawiciel** – osoba fizyczna lub prawna, która została wyznaczona na piśmie przez ADO lub podmiot przetwarzający do reprezentowania ADO lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z przepisów prawa lub niniejszego Regulaminu,
15) **Organ nadzorczy, UODO** – Urząd Ochrony Danych Osobowych, niezależny organ publiczny powołany do spraw ochrony danych osobowych,
16) **Odbiorca** - osoba fizyczną lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania, nie są uznawane za odbiorców.
17) **Strona trzecia** - osoba fizyczną lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia ADO lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe,
18) **Zgoda –** rozumiana jako zgoda osoby, której dane dotyczą - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych,
19) **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,
20) **Incydent** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu danych (na podstawie Polskiej Normy PN-ISO/IEC 27002),
21) **Zagrożenie –** potencjalna przyczyna niepożądanego incydentu, którego skutkiem mogą być straty w zasobach,
22) **Podatność –** skłonność zasobu na oddziaływanie zagrożeń,
23) **Ryzyko** – prawdopodobieństwo, że określone zagrożenie w połączeniu z podatnością doprowadzi do utraty lub zniszczenia zasobów,
24) **Analiza ryzyka** – proces identyfikacji ryzyka, określanie jego wartości, identyfikowanie zagrożeń i określanie niezbędnych zabezpieczeń w oparciu o jej wyniki,
25) **Monitorowanie –** proces weryfikacji stosowanych metod i zasad bezpieczeństwa oraz kontrola ich przestrzegania,

26) **System teleinformatyczny (system informatyczny)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
27) **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w ZTM, osoba wykonująca pracę na podstawie umowy cywilnoprawnej oraz osoba odbywająca staż lub mająca praktykę w ZTM, a także inna osoba posiadająca upoważnienie ADO do przetwarzania danych osobowych w systemie,
28) **Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych -** zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, w tym informacji wrażliwych, wewnątrz systemu informatycznego, uregulowany w Rozdziale VII Regulaminu,
29) **Zabezpieczenie danych w systemie informatycznym –** wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
30) **Uprawnienia –** nadany przez ADO i zrealizowany przez IOD i ASI zakres czynności umożliwiający dostęp do danych osobowych w określonym czasie zadaniowym (np. odczyt, wprowadzanie danych, modyfikacja),
31) **Hasło dostępu -** ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej,
32) **Identyfikator –** dowolny, jawny ciąg znaków literowych lub cyfrowych unikalny w skali ZTM, jednoznacznie identyfikujący użytkownika systemu przetwarzającego dane,
33) **Integralność danych –** właściwość zapewniająca, że dane nie zostaną zmienione lub zniszczone w sposób nieautoryzowany,
34) **Koń trojański** – program, najczęściej szkodliwy, instalujący się na komputerze bez wiedzy użytkownika, który umożliwia nieuprawnione gromadzenie, fałszowanie lub niszczenie danych,
35) **Stanowisko pracy –** wyznaczone przez ADO w uzgodnieniu z IOD i ASI – pojedyncze stanowisko robocze lub grupa stanowisk wydzielona dla realizacji określonych zadań związanych z przetwarzaniem danych osobowych,
36) **Opiekun techniczny stanowiska (grupy stanowisk) –** osoba odpowiedzialna za programowo – sprzętowe zabezpieczenie stanowiska pracy,
37) **Osoba postronna –** to każda osoba nie posiadająca upoważnienia dopuszczającego do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, nadanego przez ADO,
38) **Sieć publiczna –** sieć telekomunikacyjna niebędąca siecią wewnętrzną, służącą do świadczenia usług telekomunikacyjnych,
39) **Strefa ochronna** – określony, zdefiniowany obszar (pomieszczenie lub zespół pomieszczeń), do którego mogą mieć dostęp tylko określone osoby, wymagający odpowiednich środków zabezpieczenia i kontroli oraz upoważnień dla osób w nich przebywających.

§ 4
Deklaracja ADO

1. Niniejszy dokument wyraża zaangażowanie ADO w zakresie utrzymania odpowiedniego poziomu ochrony danych oraz określa podstawowe, przyjęte w tym obszarze, cele i strategie.
2. ADO aktywnie wspiera zapewnienie bezpieczeństwa informacji w całej jednostce, wskazując kierunki działania oraz przyjmując odpowiedzialność w zakresie bezpieczeństwa danych.

Rozdział II
RAMY PRAWNE OCHRONY DANYCH

§ 5
Przepisy prawa normujące zasady ochrony danych

1. W ZTM dane (informacje) podlegają ochronie zgodnie z zasadami zawartymi w Polityce oraz określonymi w następujących aktach prawnych:
   1) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1), zwane dalej „RODO”,
   2) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781)
   3) ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2019r. poz. 742),
   4) ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2020r. poz. 2176, z późn. zm.),
   5) ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 2070),
   6) ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2020 r. poz. 1320, z późn. zm.),
   7) rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. 2011r. Nr 159, poz. 948),
   8) rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247), zwane dalej „KRI”,
   9) rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz. U. Nr 148, poz. 973),
   10) ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2021 r. poz. 1062, z późn. zm.).
2. Podstawą normalizacyjną dokumentu Polityki są niżej wymienione Polskie Normy:

1) PN ISO/IEC 27001:2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania,
2) PN ISO/IEC 27005 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji,
3) PN-ISO/IEC 27002 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.

§ 6

Zakres funkcjonowania systemu bezpieczeństwa informacji

1. Działając na podstawie § 20 KRI, realizując Politykę, zapewnia się:
   a) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom (na podstawie PN-ISO/IEC 27001),
   b) integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany, zapewnia się dokładność i kompletność aktywów (na podstawie PN-ISO/IEC 27001),
   c) dostępność – istnieje możliwość wykorzystania danych na żądanie, w założonym czasie, przez upoważniony podmiot (na podstawie PN-ISO/IEC 27001),
   d) rozliczalność – możliwość jednoznacznego przypisania określonego działania do określonego podmiotu (procesu, systemu) oraz umiejscowienia go w czasie,
   e) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
   f) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
   g) niezawodność – zamierzone zachowania i skutki są spójne.
2. Polityka ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:
   a) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone ZTM,
   b) naruszeń przepisów prawa oraz innych regulacji,
   c) utraty lub obniżenia reputacji ZTM,
   d) strat finansowych ponoszonych w wyniku nałożonych kar,
   e) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.
3. Realizując Politykę w zakresie ochrony danych osobowych ZTM dokłada szczególnej staranności w celu ochrony interesów osób, których dane te dotyczą, a w szczególności zapewnia warunki, aby dane te były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   c) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
   d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 7

Kategorie przetwarzanych danych

1. Zasoby informacyjne w ZTM to zasoby materialne i niematerialne, w tym wszelkiego rodzaju użyteczne dane (informacje) niezbędne do skutecznego i zgodnego z przepisami prawa podejmowania decyzji.
2. Zasoby informacyjne dzielimy na:
   a) **informacje** – w szczególności bazy danych i pliki z danymi, kontrakty, umowy, dokumentacja systemowa, podręczniki użytkownika, materiały szkoleniowe, procedury, ślady audytowe, informacje zarchiwizowane, akta spraw,
   b) **system teleinformatyczny** – współdziałające ze sobą aplikacje, programy, urządzenia komputerowe, urządzenia telekomunikacyjne, nośniki informacji i inne,
   c) **zasoby lokalowe** – w szczególności budynki, pomieszczenia i inne, w których przetwarza się dane,
   d) **usługi** – w szczególności teleinformatyczne, telekomunikacyjne, ogrzewanie, zasilanie i podobne,
   e) **ludzkie** – ludzie, ich kwalifikacje, umiejętności i doświadczenie,
   f) **wartości niematerialne** – w szczególności reputacja i wizerunek ZTM.

Rozdział III
ORGANIZACJA OCHRONY DANYCH W ZTM PRZYDZIAŁ OBOWIĄZKÓW I ODPOWIEDZIALNOŚCI

§ 8

Organizacja ochrony danych

1. W ZTM za bezpieczeństwo informacji, w tym za ochronę danych osobowych odpowiada Administrator Danych Osobowych (ADO).
2. ADO powołuje w ZTM Inspektora Ochrony Danych (IOD). Jeden IOD może zostać również powołany wspólnie dla kilku jednostek organizacyjnych, o ile można z nim łatwo nawiązać kontakt z każdej z tych jednostek.
3. ADO może dodatkowo powołać w ZTM Administratora Systemu Informatycznego (ASI).
4. W związku z faktem, iż część zadań IOD i ASI pokrywa się, dopuszcza się możliwość wyznaczenia na te stanowiska jednej osoby.
5. W przypadku nie powołania Administratora Systemu Informatycznego (ASI), określone Polityką obowiązki ASI, wykonuje bezpośrednio Administrator Danych Osobowych (ADO).

§ 9

Role związane z zapewnieniem ochrony danych

1. **Administrator Danych Osobowych (ADO)** – Dyrektor ZTM:
   a) odpowiada za zgodne z prawem przetwarzanie danych osobowych w ZTM,

b) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
c) formułuje, wdraża i w razie potrzeby uaktualnia środki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
d) szacuje ryzyko i dokonuje oceny planowanych operacji przetwarzania danych osobowych, a w przypadku oszacowania wysokiego ryzyka konsultuje się z organem nadzorczym,
e) prowadzi rejestr czynności przetwarzania danych,
f) zawiera umowę powierzenia przetwarzania danych osobowych, w przypadku przekazania posiadanych danych osobowych podmiotowi przetwarzającemu,
g) zgłasza niezwłocznie organowi nadzorczemu przypadki naruszenia ochrony danych osobowych oraz zawiadamia o tym fakcie osobę, której dane dotyczą,
h) wydaje upoważnienie do przetwarzania danych osobowych – wzór upoważnienia stanowi załącznik nr 1 do Polityki,
i) odwołuje upoważnienie do przetwarzania danych osobowych - wzór odwołania upoważnienia stanowi załącznik nr 2 do Polityki.

2. Czynności, o których mowa w ust. 1, ADO dokonuje w ścisłej współpracy z IOD.

3. **Inspektor Ochrony Danych (IOD)** – wyznaczony przez ADO pracownik ZTM lub osoba zatrudniona w tym zakresie na podstawie umowy cywilnoprawnej:
a) informuje ADO, podmiot przetwarzający, pracowników i inne osoby, które z upoważnienia ADO przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO, Polityki oraz innych przepisów dotyczących ochrony danych osobowych,
b) monitoruje przestrzeganie zasad ochrony przetwarzanych danych osobowych, w tym zasad określonych Polityką,
c) udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
d) bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w ZTM i zapewnia odpowiedni poziom przeszkolenia w tym zakresie,
e) prowadzi kontrolę przetwarzania danych osobowych,
f) pełni rolę głównego arbitra merytorycznego w zakresie bezpieczeństwa danych, w tym przetwarzanych w ramach systemu informatycznego,
g) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór ewidencji stanowi załącznik nr 3 do Polityki,
h) przyjmuje od osób uzyskujących dostęp do zasobów informacyjnych ZTM oraz przetwarzających dane osobowe, oświadczenie o zapoznaniu się z Polityką, a także z RODO i innymi przepisami związanymi z ochroną danych osobowych, w tym o odpowiedzialności karnej za naruszenie ochrony danych osobowych i zachowaniu tajemnicy – wzór oświadczenia stanowi załącznik nr 4 do Polityki,
i) prowadzi wykaz osób, które zostały zapoznane z Polityką, a także z RODO i innymi przepisami związanymi z ochroną danych osobowych – wzór wykazu stanowi załącznik nr 5 do Polityki,
j) określa potrzeby w zakresie stosowanych w ZTM zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia,

k) opracowuje roczne sprawozdanie dla ADO z podjętych działań, kontroli, szkoleń, zawierające informację o stwierdzonych incydentach i ryzykach, w którym przedstawia również propozycje mające na celu zwiększenie bezpieczeństwa ochrony danych osobowych,
l) informuje ADO o zmianie przepisów prawa dotyczących szeroko rozumianej ochrony danych oraz wnioskuje do ADO o aktualizację przepisów wewnętrznych w tym zakresie,
m) w imieniu ADO, współpracuje z organem nadzorczym oraz podmiotami kontrolującymi ZTM w zakresie ochrony danych osobowych,
n) udziela na żądanie organu nadzorczego zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania, po dokonaniu przez ADO oszacowania ryzyka i oceny planowanych operacji przetwarzania danych osobowych,
o) pełni funkcję punktu kontaktowego dla UODO, w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, w przypadku oszacowania wysokiego ryzyka przetwarzania danych osobowych.

4. Osoby, których dane dotyczą, mogą bezpośrednio kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO oraz niniejszej Polityki.
5. IOD jest włączany we wszystkie sprawy dotyczące ochrony danych osobowych w ZTM, w szczególności w sprawy określone w Rozdziale VI Polityki.
6. IOD może wykonywać inne niż wynikające z Regulaminu zadania i obowiązki, pod warunkiem, że nie będą one powodowały konfliktu interesów.
7. IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
8. Obowiązki i wytyczne, o których mowa w ust. 3-7, winny zostać spełnione również przez IOD wyznaczonego przez podmiot przetwarzający.
9. ADO i podmiot przetwarzający mogą wyznaczyć jednego, wspólnego IOD.
10. ADO publikuje (na stronie internetowej, na tablicy ogłoszeń lub w innym publicznie dostępnym miejscu) dane kontaktowe IOD i zawiadamia o nich organ nadzorczy.
11. **Administrator Systemu Informatycznego (ASI)** – wyznaczony przez ADO pracownik ZTM lub osoba zatrudniona w tym zakresie na podstawie umowy cywilnoprawnej:
    a) odpowiada za funkcjonowanie systemów i sieci teleinformatycznych, realizację zadań związanych z zarządzaniem systemem informatycznym ZTM, w tym za zabezpieczenie sieci komputerowej, tj. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w ZTM w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem, ujawnieniem oraz ich utratą, zapewniając poufność, integralność i dostępność informacji przetwarzanych w systemach oraz odpowiada za usuwanie ewentualnych niezgodności z regulacjami określonymi w Polityce,
    b) zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym, zgodnie z wymogami prawa i wskazówkami IOD lub ADO,
    c) wyznacza, doskonali i rozwija wymagane ustawowo zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem, w tym współpracuje z informatykiem w zakresie wdrażania zabezpieczeń informatycznych, np.: wprowadzenie polityki haseł, zapewnienie kopii bezpieczeństwa, kontrola zgodności oprogramowania, pomoc w dostosowaniu, doborze lub zmianie oprogramowania do przetwarzania danych osobowych, aby spełniało wymagania określone obowiązującymi przepisami prawa,

d) zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
e) prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

12. **Audytor wewnętrzny** – pracownik ZTM, osoba zatrudniona w tym zakresie na podstawie umowy cywilnoprawnej lub działająca na zlecenie organu nadrzędnego (Urząd Miasta Kielce) – odpowiada za coroczne przeprowadzenie audytu bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 KRI.
13. **Użytkownik** – pracownik ZTM, osoba zatrudniona na podstawie umowy cywilnoprawnej lub inna osoba upoważniona do przetwarzania danych osobowych:
    a) chroni prawo do prywatności osób fizycznych powierzających ZTM swoje dane osobowe, poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce,
    b) zapoznaje się z zasadami określonymi w Polityce, RODO i innych przepisach związanych z ochroną danych osobowych i składa oświadczenie, o którym mowa w ust. 3 lit. h,
    c) informuje osoby odpowiedzialne za bezpieczeństwo danych o każdym zauważonym przez niego incydencie naruszenia bezpieczeństwa.
14. **Przełożony** – odpowiada za nadzór nad realizacją zadań wynikających z Polityki przez podległych pracowników.

§ 10

Odpowiedzialność za ochronę danych

1. Skuteczna ochrona zasobów informacyjnych ZTM wymaga wspólnego działania i zaangażowania wszystkich pracowników. Zarówno ADO, IOD, ASI, jak i wszyscy pracownicy są zobowiązani, odpowiednio do swoich obowiązków i zajmowanych stanowisk, do przestrzegania Polityki. Pracownicy w szczególności zobowiązani są do przestrzegania procedur opisujących zasady korzystania z haseł, procedur ochrony antywirusowej oraz procedur eksploatacji systemów informatycznych, a także do przestrzegania zakazu udostępniania hasła do swojego komputera, zakazu korzystania z nielegalnego oprogramowania oraz zakazu instalowania jakiegokolwiek oprogramowania bez zgody IOD lub ASI. Pracownicy są zobowiązani do używania zasobów informacyjnych ZTM wyłącznie do celów służbowych. Ponadto wszyscy pracownicy są zobowiązani do przestrzegania zasad ochrony informacji prawnie chronionej, w tym danych osobowych i informacji niejawnych.
2. W przypadku osób lub podmiotów, z którymi ZTM zawiera umowy cywilno-prawne, z których wynika, że będą korzystali z zasobów informacyjnych ZTM należy w zawieranej umowie wprowadzić klauzulę dotyczącą obowiązku przestrzegania postanowień Polityki a w przypadku procesorów zawrzeć umowę powierzenia przetwarzania danych osobowych. W takiej sytuacji dostęp do zasobów jest ograniczony do zakresu i okresu zdefiniowanego w umowie. W uzasadnionych przypadkach należy przeprowadzić szkolenie w zakresie Polityki a ADO lub działający w jego imieniu IOD ma możliwość przeprowadzenia audytu bezpieczeństwa informacji w jednostce zewnętrznej.
3. Odpowiedzialność za bezpieczeństwo danych ZTM obejmuje nie tylko jego siedzibę, ale także wszelkie sytuacje, w których informacje związane z działalnością ZTM są przetwarzane poza jej siedzibą. Obejmuje to w szczególności zdalny (mobilny) dostęp do sieci komputerowej ZTM, a także pracę w chmurze (cloud computing).
4. W celu zapewnienia bezpieczeństwa danych ZTM stosuje się następujące ogólne zasady:

a) **zasada przywilejów koniecznych** - każdy pracownik posiada prawo dostępu do zasobów ZTM ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu obowiązków,
b) **zasada wiedzy koniecznej** - pracownicy posiadają wiedzę o zasobach ZTM ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań,
c) **zasada asekuracji zabezpieczeń** - ochrona zasobów winna opierać się na co najmniej dwóch mechanizmach zabezpieczenia,
d) **zasada rozliczalności** – ZTM dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za powierzone im zasoby. Wszyscy użytkownicy zasobów informacyjnych ponoszą odpowiedzialność za zaniedbanie swoich obowiązków w zakresie bezpieczeństwa danych,
e) **zasada czystego biurka** – należy unikać pozostawiania dokumentów na biurku bez opieki. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych oraz informatycznych nośników danych. Zaleca się przechowywanie pod zamknięciem (najlepszym rozwiązaniem jest sejf, szafa lub inna forma zabezpieczenia) dokumentów i nośników zawierających dane wrażliwe lub krytyczne informacje służbowe.
f) **zasada czystego ekranu** – zamykanie sesji lub blokowanie komputera pozostawionego bez opieki lub czasowo nieużywanego (za pomocą mechanizmu blokowania ekranu i klawiatury kontrolowanego hasłem, tokenem lub innego podobnego mechanizmu). Po zakończonym dniu pracy komputer powinien zostać wyłączony.

Rozdział IV
PROJEKTOWANIE SYSTEMU OCHRONY DANYCH UTRZYMANIE WYMAGANEGO POZIOMU OCHRONY DANYCH

§ 11

Ochrona prywatności „by design” i „by default” Dokonanie oceny skutków przetwarzania danych Analiza ryzyka

1. Polityka chroni dane już na etapie projektowania systemu ochrony danych osobowych („by design” – uwzględnienie ochrony danych w fazie projektowania).
2. Wprowadzenie w życie założeń uregulowanych Polityką powoduje, że ochrona danych jest aktywna również domyślnie („by default” – domyślna ochrona danych), czyli bez konieczności podejmowania działań przez osoby, których dane dotyczą.
3. Elementami niezbędnymi do zapewnienia ochrony prywatności by design i by default są m.in.: minimalizacja danych, ich pseudonimizacja, kodowanie danych oraz inne zasady określone w art. 25 RODO oraz wprowadzone przepisami niniejszej Polityki.
4. Jednym z elementów zapewnienia ochrony prywatności by design i by default jest dokonanie oceny skutków przetwarzania danych.
5. Dokonanie oceny skutków przetwarzania danych jest wynikiem przeprowadzenia analizy ryzyka, które ma na celu ustalenie jakiego rodzaju dane są w posiadaniu ZTM, czy ZTM posiada dane wrażliwe oraz w jakim celu, w jaki sposób i w jakim środowisku dane są przetwarzane (szacowanie ryzyka).
6. Szacowanie ryzyka pozwala zaplanować jakiego rodzaju środki organizacyjne lub techniczne należy wprowadzić, jakie zabezpieczenia dobrać, aby dane były wystarczająco chronione.

7. Analiza ryzyka prowadzi do wskazania:
    a) działań minimalizujących możliwość naruszenia ochrony danych,
    b) osób odpowiedzialnych za realizację tych działań,
    c) terminu realizacji działań minimalizujących.
8. Przeprowadzenie procedury szacowania ryzyka, w sposób pośredni służy również odpowiedniemu przygotowaniu w ZTM:
    a) rejestru czynności przetwarzania danych osobowych,
    b) klauzul informacyjnych,
    c) klauzul o wyrażeniu zgody na przetwarzanie danych osobowych.
9. Zasoby istotne dla realizacji zadań ZTM, a w szczególności informacje i sprzęt niezbędny do ich przechowywania i przetwarzania, są narażone na różne zagrożenia, które identyfikuje się w następujących obszarach ryzyka:
    a) **naruszenie poufności** – rozumiane jako udostępnienie informacji i zasobów osobom nieupoważnionym, np. przekazanie informacji pracownikom nieupoważnionym, osobom niezatrudnionym w ZTM, zagubienie zasobu,
    b) **naruszenie dostępności** – rozumiane jako znaczne obniżenie istotnych parametrów funkcjonalnych zasobów lub utrata danych, np. zniszczenie zasobu, kradzież zasobu, a także utrata na skutek wystąpienia sił wyższych albo nieumyślnego, umyślnego lub przypadkowego działania,
    c) **naruszenie integralności** – rozumiane jako nieautoryzowana zmiana treści informacji na skutek nieumyślnego, umyślnego lub przypadkowego działania,
    d) **naruszenie autentyczności** – rozumiane jako uniemożliwienie weryfikacji informacji lub danych je opisujących,
    e) **naruszenie niezaprzeczalności** – rozumiane jako zanegowanie swego uczestnictwa w procesie wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
    f) **naruszenie rozliczalności** – rozumiane jako uniemożliwienie weryfikacji działań przez osoby biorące udział w procesach wytwarzania i przetwarzania informacji.
10. Zadaniem regulacji zawartych w Polityce jest zmniejszenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy zminimalizowanie możliwości naruszenia bezpieczeństwa zasobów informacyjnych ZTM, umożliwienie wczesnego wykrycia takiego naruszenia, zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.

§ 12

Określenie poziomu ryzyka

1. ADO, we współpracy z IOD i ASI, przeprowadza okresową (co najmniej raz w roku) analizę ryzyka dla poszczególnych aktywów (zasobów, systemów), uwzględniając formę przetwarzania danych i określa poziom ryzyka naruszenia danych osobowych (niski, średni lub wysoki). Na tej podstawie dokonuje również oceny skutków przetwarzania danych, poprzez określenie proponowanych działań minimalizujących (działań naprawczych, wprowadzenia adekwatnych zabezpieczeń organizacyjnych i technicznych), terminu ich realizacji oraz wskazanie osoby odpowiedzialnej za ich wdrożenie.
2. Zastosowane techniczne i organizacyjne środki ochrony winny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

3. Oszacowanie wysokiego poziomu ryzyka przetwarzania danych osobowych wymaga skonsultowania tego faktu z organem nadzorczym, stosując w tym zakresie art. 36 RODO. Takiej konsultacji wymaga, bez względu na wysokość poziomu ryzyka, profilowanie, przetwarzanie na dużą skalę danych szczególnej kategorii oraz monitorowanie na dużą skalę miejsc publicznych.
4. Analizę ryzyka w obszarze danych osobowych, przeprowadzoną na podstawie zasad określonych w § 11 i 12, przy uwzględnieniu identyfikacji zagrożeń (§ 13) i sposobu zabezpieczenia danych (§ 14), dokonuje się w oparciu o wzór, który stanowi załącznik nr 6 do Polityki.

§ 13

Identyfikacja zagrożeń	
Ze względu na formę przetwarzania danych osobowych	**Rodzaje możliwych zagrożeń**
Dane przetwarzane i przechowywane w formie tradycyjnej	- zdarzenie losowe (powódź, pożar), - kradzież danych, oszustwo, celowe działanie na szkodę ZTM, - zaniedbania pracowników ZTM (brak pseudonimizacji danych, niedyskrecja, udostępnienie danych osobie nieupoważnionej), - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania, - pokonanie zabezpieczeń fizycznych, włamania, - podsłuchy, podglądy w celu wyłudzenia danych, - brak rejestrowania udostępniania danych, - niewłaściwe miejsce i sposób przechowywania dokumentacji.
Dane przetwarzane i przechowywane za pomocą systemów informatycznych	- nie przydzielenie użytkownikom systemu informatycznego identyfikatorów, - niewłaściwa administracja systemem, - niewłaściwa konfiguracja systemu, - fałszowanie kont użytkowników, - kradzież danych kont, - pokonanie zabezpieczeń programowych, - zaniedbania pracowników ZTM (brak szyfrowania danych, niedyskrecja, udostępnienie danych osobie nieupoważnionej), - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania, - zdarzenie losowe, np. pożar, - niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą

	nośników informacji, komputerów przenośnych lub chmury internetowej, - naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione, - przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci, - przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci, - przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych, - brak rejestrowania zdarzeń tworzenia lub modyfikowania danych.

§ 14

Sposób zabezpieczenia danych	
Ze względu na formę przetwarzania danych osobowych	**Formy wprowadzonych zabezpieczeń**
Dane przetwarzane i przechowywane w formie tradycyjnej	- przechowywanie danych w pomieszczeniach zamykanych na klucz, - przechowywanie danych osobowych w szafach zamykanych na klucz, - przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez ADO, - zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania.
Dane przetwarzane i przechowywane za pomocą systemów informatycznych	- kontrola dostępu do systemów, - zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony, - utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację, - systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych, - składowanie nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach,

	- przydzielenie pracownikom indywidualnych kont użytkowników i haseł, - stosowanie indywidualnych haseł logowania do poszczególnych programów, - właściwa budowa hasła (zawiera litery i cyfry), - okresowe zmiany haseł, - szyfrowanie plików zawierających dane.

§ 15
Utrzymanie odpowiedniego poziomu ochrony danych
Monitorowanie zagrożeń

1. Uzupełnieniem identyfikacji i analizy ryzyka, a także niezbędną praktyką po wdrożeniu mechanizmów ochrony informacji, jest monitorowanie zagrożeń i zabezpieczeń, systematyczna weryfikacja i aktualizacja Polityki oraz stosowanych zabezpieczeń.
2. Nakłady ponoszone na zabezpieczenia muszą być poprzedzone analizą ryzyka i kosztów, adekwatnie do potencjalnych strat spowodowanych naruszeniem bezpieczeństwa.
3. Zadaniem Polityki jest zmniejszenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy:
   a) zapobieganie przypadkom naruszenia bezpieczeństwa zasobów informacyjnych ZTM,
   b) zminimalizowanie możliwości naruszenia bezpieczeństwa,
   c) umożliwienie wczesnego wykrycia zagrożeń,
   d) zminimalizowanie strat związanych z naruszeniem oraz sprawne usunięcie jego skutków.
4. Dla utrzymania odpowiedniego poziomu bezpieczeństwa danych istotne jest:
   a) systematyczne szkolenie oraz podnoszenie kwalifikacji zawodowych pracowników,
   b) okresowe wykonywanie przeglądów Polityki,
   c) przeprowadzanie planowych i doraźnych kontroli bezpieczeństwa informacji, w tym ochrony danych osobowych w ZTM,
   d) dokonywanie analizy ryzyka naruszenia bezpieczeństwa informacji,
   e) niezwłoczne przywracanie systemu bezpieczeństwa informacji do poziomu akceptowalnego, szczególnie po zgłoszeniu lub zauważeniu incydentu w tym systemie,
   f) dokonywanie sprawozdawczości z działania systemu ochrony danych,
   g) przeprowadzanie audytów bezpieczeństwa informacji.

Rozdział V

PRZETWARZANIE DANYCH OSOBOWYCH
WYKAZ MIEJSC PRZETWARZANIA I FORMY ZABEZPIECZEŃ
REJESTROWANIE CZYNNOŚCI PRZETWARZANIA DANYCH
OBOWIĄZKI PROCESORA

§ 16

Zgodność przetwarzania danych z prawem

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:
   a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
   b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
   c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO,
   d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
   e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO,
   f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
2. Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

§ 17

Rejestrowanie czynności przetwarzania danych

1. Zapewnienie poufności danych wymaga kontroli nad procesami ich przetwarzania. Nadzór nad procesami przetwarzania informacji chronionych wymaga identyfikacji rodzajów zasobów chronionych. W tym celu ADO, we współpracy z IOD, prowadzi rejestr wszystkich czynności przetwarzania danych, mających miejsce w ZTM, z zastrzeżeniem ust. 2.
2. ADO może powierzyć prowadzenie rejestru, o którym mowa w ust. 1, IOD lub innemu przedstawicielowi ADO.
3. Rejestrowanie czynności przetwarzania danych osobowych przeprowadza się w oparciu o wzór, który stanowi załącznik nr 7 do Polityki.
4. Każdy podmiot przetwarzający dane osobowe w imieniu ADO winien prowadzić „Rejestr kategorii przetwarzania danych przez procesora w imieniu administratora", którego wzór stanowi załącznik nr 8 do Polityki.
5. Rejestry, o których mowa w ust. 3 i 4, mają formę pisemną, w tym formę elektroniczną.
6. ADO oraz procesor udostępniają rejestry na żądanie organu nadzorczego.

7. Rejestry winny być okresowo (co najmniej raz w roku) przeglądane, modyfikowane i uzupełniane.

§ 18

Wykaz miejsc, w których przetwarzane są dane osobowe

1. Dane osobowe przetwarzane są w budynkach Zarządu Transportu Miejskiego zlokalizowanych na terenie miasta Kielce w następujących lokalizacjach
   1) Zarząd Transportu Miejskiego w Kielcach, Plac Niepodległości 1 – Główna siedziba
   2) Mini dworzec autobusowy: Os. Świętokrzyskie, ul. Jana Nowaka - Jeziorańskiego
   3) Mini dworzec autobusowy: Os. Ślichowice, ul. Massalskiego.
   4) Dworzec autobusowy, ul. Czarnowska 12
   5) Punkt Informacyjny przy ul. Żytniej 1,
   6) Punkt Sprzedaży Biletów w Hali Widowiskowej przy ul. Żytniej 1,
   7) Magazyn biletowy – Hala Widowiskowa ul Żytnia 1
   8) Pomieszczenie do serwisowania automatów biletowych w MPK.
   9) Składnica akt (archiwum) – ul. Sienkiewicza 76 / 42U.

Lp.	Nazwa zbioru danych	Nazwa oprogramowania (Producent)	Adres / Nr pokoju
1.	Dane osobowe kontrahentów, dokumentacja Finansowo – Księgowa	Integra / Complex – Computers	Plac Niepodległości 1
2.	Dane osobowe pracowników, dokumentacja Kadrowo – Płacowa	Enova/Soneta	Plac Niepodległości 1
3.	Dane osobowe pasażerów	Municom / R&G	Plac Niepodległości 1 / Punkty sprzedaży biletów / Dworzec autobusowy
4.	Dane osobowe pasażerów	Kielecka Karta Miejska / R&G	Plac Niepodległości 1 / Punkty sprzedaży biletów / Dworzec autobusowy / kontrola biletów
5.	Dane osobowe pasażerów	PeselNET	Plac Niepodległości 1/ Punkty sprzedaży biletów / Dworzec autobusowy / kontrola biletów
6.	Dane osobowe pracowników ZTM	Płatnik / Asseco	Plac Niepodległości 1
7.	Dane przewoźników	1C – System dworca autobusów	Plac Niepodległości 1 /

			Dworzec autobusowy
8	Opłata dodatkowa za jazdę bez ważnego biletu – dane pasażerów	Office – EXCEL/WORD	Plac Niepodległości 1 / kontrola biletów / składnica akt
9.	Wnioski o nienakładanie opłaty dodatkowej - dane pasażerów	Office – EXCEL/WORD	Plac Niepodległości 1 / kontrola biletów / składnica akt
10.	Skargi i wnioski dotyczące funkcjonowania komunikacji miejskiej	Office – EXCEL/WORD	Plac Niepodległości 1 / składnica akt
11.	Dane osobowe Przewoźników korzystających z Dworca Autobusowego	Office – EXCEL/WORD	Plac Niepodległości 1/ Dworzec autobusowy / składnica akt
12.	Wnioski o wydanie Kieleckiej Karty Miejskiej - dane pasażerów	Office – EXCEL/WORD	Plac Niepodległości 1/ Punkty sprzedaży biletów / składnica akt
13	Dane osobowe pracowników	Active Directory / Microsoft	Plac Niepodległości 1/ Dworzec autobusowy
14	Dane osobowe pracowników – kontrola dostępu	KANTECH	Dworzec autobusowy

§ 19

Dobór zabezpieczeń

ADO dobiera cele stosowania zabezpieczeń i zabezpieczenia odpowiednio do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji. Zabezpieczenia fizyczne, techniczne i organizacyjne uzupełniają się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji. W doborze celów stosowania zabezpieczeń ADO kieruje się zaleceniami Polskiej Normy PN-ISO/IEC 27002.

§ 20

Formy zabezpieczenia miejsc, w których przetwarzane są dane osobowe

1. Wejścia do budynku ZTM zabezpieczone winny być przynajmniej zamkami drzwiowymi.
2. Poszczególne pokoje, w których odbywa się przetwarzanie danych i ich składowanie muszą być wyposażone w niezależne zamki i muszą być zamykane podczas nieobecności

pracownika. Po zakończeniu pracy osoba zamykająca pomieszczenie zabiera klucze i zabezpiecza je we własnym zakresie.
3. Stanowiska komputerowe w pomieszczeniach, gdzie mogą przebywać osoby nieupoważnione do przetwarzania danych osobowych (np. interesanci albo inni pracownicy ZTM) winny być umieszczone w sposób, który uniemożliwi takim osobom wgląd do tych danych. W pokoju, do którego dostęp mają petenci monitory komputerowe ustawione są w ten sposób, by interesanci nie widzieli zapisów na ekranie.
4. W przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacze ekranu lub blokowanie systemu, których dezaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.
5. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.

§ 21

Zasady udzielania dostępu do danych osobowych

1. Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa, lub na podstawie wniosku, o którym mowa w § 22, jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.
2. Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami Polityki, RODO i innymi przepisami związanymi z ochroną danych osobowych, a w przypadku osób upoważnionych do dostępu do tych danych na podstawie ogólnie obowiązujących przepisów (np. przedstawicieli organów kontroli, wizytatorów), po konsultacji z IOD.
3. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu, o którym mowa w § 9 ust. 3 lit. h.
4. Dostęp do przetwarzania danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie, o którym mowa w § 9 ust. 1 lit. h, nadane przez ADO.

§ 22

Wniosek o udostępnienie danych

1. Udostępnienie danych może nastąpić na pisemny wniosek, zawierający następujące elementy:
   - adresat wniosku (administrator danych),
   - wnioskodawca,
   - podstawa prawna (wskazanie potrzeby),
   - wskazanie przeznaczenia,
   - zakres informacji.
2. ADO odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.
3. Powierzenie przetwarzania danych może nastąpić wyłącznie w drodze pisemnej umowy, o której mowa w § 23.

§ 23

Powierzenie przetwarzania danych procesorowi
Obowiązki procesora

1. Dane osobowe powierza się wyłącznie podmiotowi (procesorowi), który spełnia wymagania przepisów normujących kwestię bezpieczeństwa informacji, w tym RODO i Polityki.
2. Podmiot, któremu powierza się dane osobowe powinien posiadać środki (techniczne i organizacyjne) zabezpieczające zbiór powierzonych danych osobowych.
3. Z podmiotem, któremu zostają powierzone dane osobowe zawiera się pisemną umowę powierzenia przetwarzania danych osobowych, która winna określać zakres i cel takiego powierzenia oraz zapewniać by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy.
4. Umowa powierzenia może stanowić część (klauzulę) innej umowy cywilnoprawnej.
5. Procesor nie może powierzać dalej przetwarzania danych osobowych bez zgody ADO. ADO może zezwolić na podpowierzenie danych osobowych, ale wyłącznie podmiotom wskazanym w umowie lub w innym pisemnym dokumencie.
6. ADO może w umowie zastrzec prawo do kontroli (audytu bezpieczeństwa) powierzonych danych w jednostce, której dane powierzył, a także do przeprowadzenia szkolenia przedstawicieli i pracowników procesora z przepisów RODO i Polityki.
7. Obowiązkiem procesora, co również winno zostać zastrzeżone w umowie powierzenia przetwarzania danych osobowych, jest prowadzenie rejestru wszelkich kategorii czynności przetwarzania, dokonywanych w imieniu ADO, według wzoru, o którym mowa w § 17 ust. 4. Procesor ma obowiązek udostępnić taki rejestr na żądanie UODO.
8. Procesor ma również obowiązek powołać własnego IOD, jeżeli zaistnieje przynajmniej jeden z czynników, o których stanowi art. 37 ust. 1 RODO.
9. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych ADO zadecyduje czy procesor ma usunąć czy zwrócić wszelkie dane osobowe oraz ich kopie, chyba że przepisy prawa nakazują przechowywanie tych danych osobowych.
10. Procesor w razie stwierdzenia, iż doszło do naruszenia ochrony danych osobowych zgłasza ten fakt bezpośrednio ADO, przy czym organ nadzorczy będzie mógł egzekwować stosowanie RODO bezpośrednio w stosunku do procesora.
11. Jeżeli procesor naruszy przepisy RODO, przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora danych w odniesieniu do tego przetwarzania.
12. Procesor oraz każda osoba działająca z upoważnienia procesora lub ADO, mająca dostęp do danych osobowych, przetwarza je wyłącznie na polecenie ADO, chyba że wymaga tego przepis prawa.

§ 24

Przetwarzanie danych wrażliwych

1. Zabrania się przetwarzania danych wrażliwych.
2. Przetwarzanie danych wrażliwych dopuszczalne jest jedynie w sytuacjach wskazanych w art. 9 ust.2-4 RODO, tj. jeżeli spełniony jest jeden z poniższych warunków:
   a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie danych wrażliwych w jednym lub kilku konkretnych celach, chyba że przepisy prawa przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania danych wrażliwych,
   b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez ADO lub osobę, której dane dotyczą, w dziedzinie prawa

pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone przepisami prawa, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą,

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami, oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą,
e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,
g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie przepisów prawa, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,
h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie przepisów prawa lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3,
i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie przepisów prawa, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę służbową (zawodową),
j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie przepisów prawa, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3. Dane wrażliwe mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h, jeżeli są przetwarzane przez - lub na odpowiedzialność - pracownika podlegającego obowiązkowi zachowania tajemnicy służbowej (zawodowej) na mocy przepisów prawa lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy przepisów prawa.
4. W sytuacji określonej w ust. 2 lit. j, jeżeli jest to możliwe ze względu na cel przetwarzania i jeżeli przepisy prawa na to pozwalają, dane winny zostać poddane anonimizacji.

§ 25

Przetwarzanie danych osobowych
dotyczących wyroków skazujących i naruszeń prawa

Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa, na podstawie art. 6 ust. 1 RODO, wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone przepisami prawa przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

Rozdział VI

OBOWIĄZKI INFORMACYJNE ZTM
UPRAWNIENIA OSÓB, KTÓRYCH DANE DOTYCZĄ

§ 26
Polityka informacyjna ZTM z zakresu ochrony danych osobowych

1. ZTM prowadzi politykę informacyjną z zakresu ochrony danych osobowych, zgodnie z wytycznymi RODO. W tym celu m.in. podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich niezbędnych informacji.
2. Informacji, o których mowa w ust. 1, udziela się co do zasady na piśmie, w tym elektronicznie (e-mailem). Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
3. Obowiązki informacyjne wykonywane są bez zbędnej zwłoki, nie później niż w terminie miesiąca od otrzymania żądania. W przypadku skomplikowanego charakteru żądania lub dużej liczby żądań, ADO może wydłużyć termin załatwienia takiej sprawy do dwóch miesięcy.
4. Informacje z zakresu ochrony danych oraz komunikacja i działania podejmowane na podstawie RODO i Polityki są wolne od opłat.
5. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, ADO może:
   a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań,
   b) odmówić podjęcia działań w związku z żądaniem.
6. Na elementy przejrzystej polityki informacyjnej ZTM z zakresu ochrony danych osobowych składa się m.in. opracowanie na podstawie RODO i Polityki:
   a) klauzuli wyrażenia zgody na przetwarzanie danych osobowych,
   b) klauzul informacyjnych,
   c) zasad określających prawa do:
      - dostępu do własnych danych osobowych,
      - sprostowania danych,
      - usunięcia danych (tzw. „prawo do bycia zapomnianym”),
      - ograniczenia przetwarzania,
      - przenoszenia danych,
      - sprzeciwu.

§ 27

Wyrażenie zgody na przetwarzanie danych osobowych

1. Dane osobowe w ZTM mogą być przetwarzane na podstawie zgody osoby, której dane dotyczą, z zastrzeżeniem wyjątków określonych w ust. 7.
2. Zgodę na przetwarzanie danych osobowych dziecka składają opiekunowie prawni dziecka.
3. Uzyskanie zgody na przetwarzanie danych osobowych jest obowiązkowe, m.in. w przypadku umieszczenia na tablicy ogłoszeń lub stronie internetowej wizerunku osoby (np. pracownika). Jednakże zgoda nie jest wymagana, gdy wizerunek osoby stanowi jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.
4. Zgoda na przetwarzanie danych osobowych, może mieć charakter odrębnego oświadczenia lub klauzuli stanowiącej integralny element innego dokumentu ZTM.
5. Przykładowy wzór zgody na przetwarzanie danych osobowych, stanowi załącznik nr 9 do Polityki.
6. Osoba składająca zgodę na przetwarzanie danych osobowych ma prawo w dowolnym momencie wycofać tą zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
7. Wymóg wyrażenia zgody na przetwarzanie danych osobowych, nie rozciąga się na określone przepisami dane pracowników ZTM, obejmujące: imię, nazwisko, stanowisko służbowe, służbowy numer telefonu czy też służbowy adres e-mailowy. Dane te mogą również bez zgody pracowników pojawić się na stronie internetowej ZTM.

§ 28
Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego

1. W przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat.
2. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

§ 29

Klauzule informacyjne

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, ZTM podczas pozyskiwania danych osobowych podaje jej wszystkie wymagane informacje, określone w załączniku nr 10 do Polityki, w formie tzw. klauzuli informacyjnej.
2. Mając na uwadze różne cele przetwarzania danych osobowych w ZTM, winno się wyróżnić tyle klauzul informacyjnych, ile uda się wyróżnić celów przetwarzania danych osobowych.
3. Klauzule informacyjne winny zostać przedstawione w taki sposób, aby odbiorca mógł się z nimi bez trudu zapoznać. Przykładowe sposoby prezentacji (publikowania) klauzul informacyjnych:
   a) umieszczenie na tablicy ogłoszeń,
   b) zamieszczenie na stronie internetowej (najlepiej w formie odrębnej dedykowanej zakładki),
   c) na dokumencie zgody na przetwarzanie danych osobowych,
   d) na wzorach dokumentów, które odbiorca klauzuli będzie wypełniał,
   e) jeżeli klauzule zostały opublikowane na stronie internetowej, wówczas dodatkową formę informacyjną może stanowić podanie na druku zgody na przetwarzanie danych

osobowych oraz na wzorach dokumentów, które odbiorca klauzuli będzie wypełniał, odpowiedniego linku do tej strony internetowej.

§ 30
Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, ADO podaje osobie, której dane dotyczą, następujące informacje:
   a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
   b) dane kontaktowe IOD,
   c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania,
   d) kategorie odnośnych danych osobowych,
   e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   f) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
2. Poza informacjami, o których mowa w ust. 1, ADO podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:
   a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO - prawnie uzasadnione interesy realizowane przez ADO lub przez stronę trzecią,
   c) informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   e) informacje o prawie wniesienia skargi do organu nadzorczego,
   f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych,
   g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
3. Informacje, o których mowa w ust. 1 i 2, ADO podaje:
   a) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych,

b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą, lub
c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.

4. Jeżeli ADO planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 1 i 2.
5. Ust. 1- 4 nie mają zastosowania, gdy - i w zakresie, w jakim:
   a) osoba, której dane dotyczą, dysponuje już tymi informacjami,
   b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile obowiązek, o którym mowa w ust. 1, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach ADO podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie,
   c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane przepisami prawa przewidującymi odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą, lub
   d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy służbowej (zawodowej) przewidzianym w przepisach prawa, w tym ustawowym obowiązkiem zachowania tajemnicy.
6. ADO w celu wypełnienia obowiązku określonego w ust. 1-5, może zastosować – w postaci klauzul informacyjnych – zasady określone w § 30 ust. 2-3.

§ 31

Prawo dostępu przysługujące osobie, której dane dotyczą

1. Każda osoba fizyczna, której dane dotyczą, jest uprawniona do uzyskania od ADO potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz informacji: o celach przetwarzania, kategorii danych osobowych, o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione (w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych), o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu, o prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania, o prawie wniesienia skargi do organu nadzorczego, o źródle danych - jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą oraz o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
2. ADO dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. Prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych osób.

§ 32
Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

§ 33
Prawo do usunięcia danych („prawo do bycia zapomnianym")
Procedura usunięcia danych

1. Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia dotyczących jej danych osobowych, a ADO ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
   b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
   c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne, prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania,
   d) dane osobowe były przetwarzane niezgodnie z prawem,
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega ADO,
   f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w § 29 Polityki.
2. ADO - jeśli prośba o usunięcie danych zostanie rozpatrzona pozytywnie - ma również obowiązek (w przypadku wcześniejszego upublicznienia danych osobowych, np. na stronie internetowej) zgłosić takie żądanie również pozostałym administratorom, którzy przetwarzają dane osoby, która skorzystała z prawa do bycia zapomnianym. Usunięte mają być zarówno kopie tych danych jak i wszelkie odnośniki do nich, które znajdują się w innych miejscach.
3. Czynność, o której mowa w ust. 2, powinna zostać wykonana jedynie w przypadku, kiedy jej przeprowadzenie nie będzie wymagało nadmiernych środków technicznych oraz kosztów.
4. Z prawa do bycia zapomnianym mają możliwość skorzystać osoby, które same wyraziły zgodę na przetwarzanie własnych danych osobowych, lub kiedy informacje te zostały pozyskane przez ADO w sposób inny niż od osoby, której dane dotyczą.
5. Nie można skorzystać z prawa do bycia zapomnianym, jeżeli przetwarzanie jest niezbędne:
   a) w celu korzystania z prawa do wolności wypowiedzi i informacji,
   b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na podstawie przepisów prawa lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO.
   c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,
   d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych,
   e) do ustalenia, dochodzenia lub obrony roszczeń.

6. W przypadku kiedy ADO ustali, że wniosek o usunięcie danych osobowych jest bezzasadny, może on odmówić jego rozpatrzenia - za każdym jednak razem informując wnioskującego o tym fakcie (wraz z uzasadnieniem).
7. Procedura usunięcia danych:
   1) ADO lub wyznaczony przez niego pracownik ZTM, we współpracy z IOD, po przeanalizowaniu zasadności wniosku o usunięcie danych oraz po rozważeniu, czy nie zaistniały przesłanki określone w ust. 5, dokonuje fizycznego usunięcia danych osobowych, korzystając ze wszystkich dostępnych środków technicznych i organizacyjnych.
   2) Sposób usunięcia danych jest uzależniony, w szczególności od: rodzaju nośnika, rodzaju dokumentu, miejsca jego przechowywania oraz istotności dla dalszego korzystania z nośnika, dokumentu.
   3) Usunięcie danych polega w szczególności na:
      a) fizycznym, trwałym zniszczeniu danych, wraz z nośnikami, w stopniu uniemożliwiającym ich późniejsze odtworzenie,
      b) pozbawieniu danych osobowych cech identyfikujących osobę fizyczną (anonimizacja danych).
   4) Z procedury usunięcia danych osobowych należy sporządzić protokół, który zawiera:
      a) informację jakiej kategorii dane zostały usunięte,
      b) z jakich źródeł (nośników, dokumentów, systemów, ewidencji itp.) usunięto dane osobowe,
      c) wskazanie sposobu usunięcia (fizyczne zniszczenie, pseudonimizacja),
      d) datę zniszczenia,
      e) podpisy osób dokonujących usunięcia danych osobowych (przedstawicieli komisji ds. usunięcia danych), IOD oraz akceptację ADO.
   5) O usunięciu danych powiadamia się korzystającego z prawa do bycia zapomnianym (w sposób wskazany we wniosku, a przy braku konkretnego wskazania – pisemnie). Do informacji tej można załączyć kopię protokołu usunięcia danych osobowych (o ile nie narusza to praw i wolności innych osób).
   6) Terminy określone w § 26 ust. 3 Polityki stosuje się odpowiednio.

§ 34
Prawo do ograniczenia przetwarzania

1. Osoba, której dane dotyczą, ma prawo żądania od ADO ograniczenia przetwarzania w następujących przypadkach, gdy:
   a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych - na okres pozwalający ADO sprawdzić prawidłowość tych danych,
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
   c) ADO nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
   d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
2. Przykładowe metody pozwalające ograniczyć przetwarzanie danych:
   a) czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania,
   b) uniemożliwienie użytkownikom dostępu do wybranych danych,

c) czasowe usunięcie opublikowanych danych ze strony internetowej.

3. W zautomatyzowanych zbiorach danych przetwarzanie należy zasadniczo ograniczyć środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane.
4. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
5. Przed uchyleniem ograniczenia przetwarzania ADO informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.
6. Organ nadzorczy posiada uprawnienia naprawcze w zakresie ograniczenia przetwarzania danych osobowych, a są to m.in.: wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania, oraz nakazanie ograniczenia przetwarzania danych.

§ 35
Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

ADO informuje o sprostowaniu (§ 32 Polityki), usunięciu danych osobowych (§ 33 Polityki) lub ograniczeniu przetwarzania (§ 34 Polityki) , których dokonał zgodnie z zapisami RODO i Polityki, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

§ 36
Prawo do przenoszenia danych

1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, dane osobowe jej dotyczące, które dostarczyła ADO, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony ADO, któremu dostarczono te dane osobowe, jeżeli:
   a) przetwarzanie odbywa się na podstawie zgody,
   b) przetwarzanie odbywa się w sposób zautomatyzowany.
2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez ADO bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
3. Głównym celem uregulowanego w ust. 1 prawa do przenoszenia danych jest ułatwienie zamiany jednego dostawcy usług na innego.
4. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.
5. **Istotnym dla działań podejmowanych przez ZTM, w ramach jej statutowych obowiązków, jest fakt, iż prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO.**

§ 37
Prawo do sprzeciwu

1. Każdej osobie, której dane są przetwarzane, przysługuje prawo ich kontroli. Wyraża się ono, między innymi, możliwością wniesienia w dowolnym momencie sprzeciwu – z przyczyn związanych ze szczególną sytuacją tej osoby - wobec przetwarzania dotyczących jej danych osobowych opartego na zgodzie, w tym profilowaniu.
2. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, osoba, której dane dotyczą, ma prawo wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
3. W związku z korzystaniem z usług społeczeństwa informacyjnego osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.
4. Jeżeli osoba, o której mowa w ust. 1, skorzysta z przysługującego jej prawa sprzeciwu, ADO nie może dalej przetwarzać tych danych osobowych, chyba że ADO wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
5. Informacja o przysługującym osobie prawie do sprzeciwu winna znaleźć się w treści klauzuli informacyjnej, o której mowa w § 29 Polityki, lub zostać przekazana w inny wyraźny sposób.

§ 38

Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach Profilowanie

1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:
   a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a ADO,
   b) jest dozwolona przepisami prawa,
   c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
3. W przypadkach, o których mowa w ust. 2 lit. a i c, ADO wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.
4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, chyba że istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

§ 39

Rejestr skarg

Dla transparentności podejmowanych przez ADO działań, jak również w celu poznania skali problemów związanych z ochroną danych osobowych, IOD prowadzi rejestr wszystkich skarg dotyczących problematyki ochrony danych osobowych.

Rozdział VII
INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 40

Ogólne zasady przetwarzania danych osobowych w systemach informatycznych

1. Przetwarzanie danych osobowych w systemach informatycznych ZTM odbywa się zgodnie z obowiązującymi przepisami w zakresie ochrony danych, a w szczególności zgodnie z RODO, KRI i niniejszą Polityką.
2. Osobą odpowiedzialną za całokształt zadań związanych z eksploatacją, utrzymaniem i przetwarzaniem informatycznych systemów ZTM, służących do przetwarzania danych osobowych jest ADO.
3. ADO w szczególności odpowiedzialny jest za analizę celowości uruchomienia stanowiska do przetwarzania danych osobowych w systemach informatycznych ZTM oraz za zaakceptowanie i przekazanie do ASI wniosków o założenie stanowiska, przydzielenie lub zlikwidowanie konta użytkownikowi stanowiska, przydzielenie zasobów użytkownikowi stanowiska, wygenerowanie pierwszego hasła dostępowego.
4. ADO realizuje zadania, wynikające z niniejszego rozdziału, przy pomocy IOD, ASI oraz zatrudnionych w ZTM pracowników. W przypadku niepowołania ASI, obowiązki wynikające z niniejszego rozdziału wykonuje ADO bezpośrednio lub przy pomocy upoważnionych przez niego osób.
5. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemach informatycznych ZTM, służących do przetwarzania danych osobowych jest ASI, współpracujący w tym zakresie z IOD.
6. Wszyscy pracownicy, lub inni użytkownicy (osoby upoważnione), dopuszczeni do przetwarzania danych osobowych w systemach informatycznych ZTM odpowiedzialni są za przestrzeganie zasad opisanych w Polityce, w szczególności określonych niniejszym Rozdziałem, w zakresie ochrony haseł, wykonywania kopii bezpieczeństwa własnych zasobów, stosowania oznakowanych nośników magnetycznych, szyfrowania plików oraz profilaktyki antywirusowej.
7. Opiekun techniczny stanowiska odpowiedzialny jest za zainstalowanie (odinstalowanie) stanowiska oraz wykonywanie funkcji serwisowych.
8. Do przetwarzania danych osobowych w systemie informatycznym ZTM mogą być dopuszczone jedynie osoby, które:
   1) zostały przeszkolone w zakresie ochrony danych osobowych – złożyły stosowne oświadczenie, o którym mowa w § 9 ust. 3 lit. h,
   2) zostały przeszkolone w zakresie obsługi sprzętu komputerowego, programów i aplikacji,

3) posiadają pisemne upoważnienie ADO, o którym mowa w § 9 ust. 1 lit. h.

9. Przetwarzanie danych osobowych w systemach informatycznych ZTM jest możliwe tylko przez uprawnione osoby, w wyznaczonym przez ADO obszarze (budynku, pomieszczeniu lub wydzielonej części pomieszczenia) podlegającym ochronie i zabezpieczeniu.
10. Udostępnianie danych osobowych przetwarzanych w systemach informatycznych ZTM może odbywać się tylko za zgodą ADO na podstawie pisemnego wniosku, zweryfikowanego przez IOD. Przepisy § 22 oraz Rozdziału VI Polityki stosuje się odpowiednio.
11. Wykorzystanie danych osobowych przetwarzanych w systemie informatycznym ZTM możliwe jest wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione, a przechowywane w postaci umożliwiającej identyfikację osób, które dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 41

Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym

Tryb nadawania uprawnień do przetwarzania danych osobowych w systemie informatycznym ZTM wygląda następująco:

1) wniosek o nadanie uprawnień do przetwarzania danych osobowych w systemie informatycznym przygotowuje bezpośredni przełożony i kieruje do akceptacji ADO, który przekazuje wstępnie zaakceptowany wniosek IOD do zweryfikowania,
2) ADO (po weryfikacji wniosku przez IOD) nadaje upoważnienie do przetwarzania danych osobowych osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych,
3) we wniosku wskazuje się w szczególności, do jakich zbiorów, rodzajów danych i systemów informatycznych ZTM użytkownik ma mieć dostęp i w jakim zakresie (wprowadzanie, akceptacja odczyt i inne),
4) wnioskom nadaje się kolejne numery porządkowe,
5) wzór wniosku stanowi załącznik nr 11 do Polityki,
6) IOD we wniosku akceptuje spełnienie podstawowych wymagań i szkoleń oraz zakres uprawnień w dostępie do systemów informatycznych ZTM,
7) IOD w przypadku uwag, np.: gdy użytkownik nie został zapoznany z przepisami o ochronie danych osobowych, przekazuje niezaakceptowany wniosek do ADO. We wniosku dokonuje adnotacji, w której podaje przyczynę odmowy zatwierdzenia wniosku,
8) IOD w przypadku pozytywnej weryfikacji i akceptacji wniosku przez ADO, dokonuje aktualizacji Ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w § 9 ust. 3 lit. g, oraz stosownego wpisu w Ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym, o której mowa w § 42,
9) po przeprowadzeniu procedury dopuszczenia pracownika na podstawie pisemnego wniosku, ASI zakłada konto (chronione systemem antywirusowym), nadaje unikalny (niepowtarzalny) identyfikator użytkownikowi systemów informatycznych ZTM (ID) i określone uprawnienia, na podstawie wnioskowanego (stosownego) zakresu uprawnień do pracy w systemie informatycznym,
10) użytkownik systemu w obecności ASI uwierzytelnia się w systemie,
11) użytkownik zmienia hasło nadane mu przez ASI i rozpoczyna pracę w aplikacji,

12) w przypadku zmiany jakichkolwiek danych we wniosku, a szczególnie w przypadku likwidacji konta przełożony użytkownika jest zobowiązany złożyć do ADO nowy wniosek zawierający uaktualnione dane, bądź wniosek o zamknięcie lub likwidację konta,
13) w przypadku likwidacji konta, identyfikator ulega zablokowaniu i nie może być ponownie wykorzystany,
14) identyfikatory nadane w trybie rejestracji użytkownika są wpisywane do Ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym, o której mowa w § 42, oraz w upoważnieniu do przetwarzania danych osobowych, o którym mowa w § 9 ust. 1 lit. h,
15) w przypadku stwierdzenia niezgodnego z treścią wniosku wykorzystania konta, ASI jest uprawniony, po uzgodnieniu z ADO i IOD, do jego zamknięcia.

§ 42

Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym

1. Ewidencję osób upoważnionych i zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym ZTM prowadzi IOD, w imieniu ADO.
2. Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych ZTM uaktualniana jest na bieżąco stosownie do składanych wniosków.
3. Ewidencja winna zawierać:
   1) imię i nazwisko osoby upoważnionej,
   2) datę nadania i datę ustania uprawnień (ewentualnie numer upoważnienia),
   3) zakres upoważnienia do przetwarzania danych osobowych,
   4) identyfikator indywidualny (ID).
4. Wzór Ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym stanowi załącznik nr 12 do Polityki.

§ 43

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
Przydział haseł dla użytkowników systemu informatycznego i częstotliwość ich zmiany

1. Użytkownicy systemu informatycznego przetwarzania danych osobowych są zobowiązani chronić przed nieuprawnionym wykorzystywaniem wszelkie znane im lub będące w ich posiadaniu dane i urządzenia umożliwiające dostęp do tych danych oraz zasobów sieci komputerowej. Oznacza to przede wszystkim zakaz ujawniania haseł dostępu, zakaz udostępniania plików zawierających hasła, klucze szyfrujące itd.
2. Po otrzymaniu od ASI hasła użytkownik powinien niezwłocznie zmienić te hasła na własne, znane tylko sobie. Hasła te powinny spełniać następujące wymagania:
   1) minimalna długość hasła powinna wynosić 8 znaków,
   2) hasło powinno składać się z małych i dużych liter, cyfr i przynajmniej jednego znaku specjalnego (nie będącego literą ani cyfrą),
   3) nie należy używać wyrazów występujących w słownikach, nawet jeśli zostaną uzupełnione innymi znakami,
   4) nie należy używać żadnych wyrazów lub liczb występujących w danych personalnych użytkownika.

3. Haseł nie wolno nigdzie zapisywać, należy je zapamiętać i zmieniać co najmniej jeden raz w miesiącu.
4. Posługiwanie się danymi identyfikującymi lub uwierzytelniającymi należącymi do innego użytkownika w celu dostępu do zasobów sieci komputerowej na jego konto lub podejmowania jakichkolwiek innych działań (a zwłaszcza wykorzystanie podpisu elektronicznego) w jego imieniu jest zabronione.
5. Monitory komputerów przetwarzających dane osobowe ustawiane są w sposób uniemożliwiający wgląd w dane osobowe oraz odczytanie hasła osobom postronnym.

§ 44

Bezpieczeństwo haseł dostępu

1. Odbiór hasła dla użytkowników systemu informatycznego odbywa się tylko osobiście.
2. Dostęp do komputera odbywa się wyłącznie po wpisaniu hasła, co wyklucza nieupoważnionych użytkowników.
3. ASI przechowuje w opieczętowanych kopertach hasła systemowe. Koperty są zabezpieczone przed dostępem osób postronnych a ich otwarcie może nastąpić wyłącznie komisyjnie w obecności ASI, IOD lub innej osoby upoważnionej przez ADO.

§ 45

Rozpoczynanie, zawieszanie i zakończenie pracy

1. Pierwsze zalogowanie w systemach informatycznych ZTM polega na wpisaniu hasła otrzymanego od ASI.
2. Zakończenie pracy w systemie informatycznym polega na wylogowaniu i wyłączeniu komputera.
3. W przypadku pozostawienia stacji roboczej bez nadzoru, użytkownik powinien wylogować się z systemu informatycznego służącego do przetwarzania danych.
4. W przypadku pozostawienia stacji roboczej nie użytkowanej (powyżej 10 min.) należy użyć funkcji blokującej stanowisko komputerowe.
5. W przypadku, gdy dostęp do pomieszczenia mogą mieć osoby postronne, opuszczając pomieszczenie należy wylogować się z systemów informatycznych ZTM.

§ 46

Procedury tworzenia kopii zapasowych i kopii awaryjnych

1. Na potrzeby zachowania ciągłości działania systemów informatycznych ZTM i utrzymania integralności danych wykonuje się co miesięczne kopie zapasowe zbioru danych i oprogramowania systemowego. Kopie danych wykonywane są na dyskach magnetycznych i są przenoszone na zewnętrzne nośniki magnetyczne. Kopie zbiorów podlegają zabezpieczeniu w wyznaczonym pokoju, w zamykanej metalowej szafie, do której dostęp mają jedynie ASI, IOD i upoważnieni pracownicy.
2. Opis nośników magnetycznych z kopiami zapasowymi powinien zawierać następujące dane:
   1) system (nazwa systemu),
   2) data (dd.mm.yyyy),
   3) uwagi,
   4) podpis,

oraz powinny być zabezpieczone przed nieumyślnym skasowaniem.
3. Kopie awaryjne wykonuje ASI na nośniku magnetycznym przy pomocy programów standardowych po każdej zmianie konfiguracji systemu oprogramowania.
4. ASI indywidualnie ustala zasady, częstotliwość i zakres wykonywania kopii awaryjnych dla systemów przetwarzania danych osobowych ZTM.

§ 47

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Systemy ochrony zastosowane w systemie informatycznym przetwarzającym dane osobowe nie powinny dopuszczać możliwości zainfekowania wirusami i programami, których celem jest uzyskanie nieuprawnionego dostępu do serwerów i stacji roboczych (np. wirusem typu „koń trojański").
2. ASI wykorzystuje następujące funkcje systemowe dla zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu:
   1) identyfikacja użytkowników korzystających z zasobów systemu,
   2) uwierzytelnienie użytkowników,
   3) kontrola praw dostępu do usług i zasobów systemu,
   4) rejestracja i śledzenie informacji o dostępach lub próbach dostępu do zasobów i usług systemu,
   5) rejestracja i śledzenie komunikatów o błędach w pracy systemu,
   6) szyfrowanie i uwierzytelnianie informacji przesyłanych pomiędzy systemem, a siecią,
   7) wykrywanie obecności fałszywego oprogramowania w danych wpływających do systemu z sieci,
   8) kontrola integralności oprogramowania zainstalowanego w systemie.

§ 48

Metody i częstotliwość sprawdzania obecności i usuwania wirusów

1. Celem zabezpieczenia dysków (komputerów) przetwarzających dane osobowe w sieci komputerowej przed atakami zewnętrznych wirusów komputerowych, ASI instaluje i aktualizuje program antywirusowy.
2. ASI wykonuje codziennie aktualizację programu antywirusowego poprzez skonfigurowanie programu stacji roboczej w taki sposób, by automatyczne pobierał on najnowsze wersje szczepionek z serwerów producenta oprogramowania.
3. Na każdej stacji roboczej wykorzystywanej do przetwarzania danych osobowych w systemach informatycznych ZTM wymagane jest zainstalowanie indywidualnego programu antywirusowego wraz z aktywnym modułem do bieżącego monitorowania wirusów (ze szczególnym uwzględnieniem wirusów typu „koń trojański") oraz zabezpieczenia przed działaniem programów, których celem jest uzyskanie nieuprawnionego dostępu do tych stacji roboczych.
4. W przypadku, gdy do przetwarzania danych osobowych wykorzystuje się komputery PC pracujące również w innych systemach lub sieciach przed rozpoczęciem przetwarzania danych osobowych należy bezwzględnie dokonać kontroli antywirusowej w komputerze.

5. Należy systematycznie przeprowadzać kontrolę antywirusową całego systemu programem dostarczonym przez ASI.
6. Zabrania się umieszczania w urządzeniach odczytujących dane z nośników rozprowadzanych z gazetami, materiałami reklamowymi itp.
7. W przypadku, gdy zachowanie systemu komputerowego odbiega od normy (np.: komunikaty o błędach, nieoczekiwane zniknięcie lub pojawianie się plików lub katalogów, spowolniona praca systemu, dziwne lub niezrozumiałe informacje pojawiające się na ekranie itp.) należy również przeprowadzić kontrolę antywirusową systemu.
8. Każdy nośnik danych używany do przenoszenia danych pomiędzy stanowiskami komputerowymi, należy sprawdzić programem antywirusowym przed odczytaniem danych.

§ 49

Postępowanie w przypadku ujawnienia lub podejrzenia istnienia wirusa

1. Jeśli program antywirusowy stwierdzi istnienie wirusa na nośniku danych, taki nośnik należy natychmiast wyjąć z czytnika (czytnika CD-ROM, gniazda USB, itp.), wyraźnie oznaczyć i przekazać nośnik ASI. Następnie należy przeprowadzić kontrolę antywirusową całego systemu.
2. Jeśli program antywirusowy stwierdzi obecność wirusa w systemie należy, jeśli to możliwe, zezwolić programowi antywirusowemu na usunięcie wirusów. Jeśli program antywirusowy nie będzie mógł usunąć wirusów nie niszcząc części lub całości zbioru zainfekowanego wirusem, należy przerwać działanie programu antywirusowego i natychmiast zgłosić ten fakt ASI.

§ 50

Sposób i miejsce przechowywania elektronicznych nośników informacji zawierających dane osobowe Sposoby postępowania z wydrukami zawierającymi dane osobowe

1. Zasady przechowywania nośników informacji:
   1) nośniki zawierające kopie bieżące danych osobowych są przechowywane w odpowiednim, wyznaczonym pomieszczeniu, do którego mają dostęp jedynie uprawnieni pracownicy ZTM oraz ASI i IOD,
   2) kopie zapasowe i kopie awaryjne – oznakowane odmiennie od kopii bieżących przechowywane są w innym wyznaczonym pomieszczeniu, zgodnie z zapisami § 46 Polityki,
   3) miejsce składowania danych z backupów znane jest wyznaczonym pracownikom, ASI i IOD,
2. Zasady odnoszące się do stanowisk komputerowych:
   1) wydruku danych z sytemu należy dokonywać tylko w sytuacjach niezbędnych,
   2) wytworzone wydruki i dokumenty zawierające dane osobowe, niewykorzystywane w pracy bieżącej, powinny być niszczone w niszczarkach lub po zaewidencjonowaniu – przechowywane w szafie użytkownika,
   3) wydruki z danymi osobowymi powinny być zabezpieczone przed dostępem osób postronnych – przechowywane w zamykanych szafach lub niszczone,

4) wydruki wykonywane w celach weryfikacji wewnętrznej, po wykorzystaniu należy bezwzględnie niszczyć,
5) zabrania się wykonywania wydruków danych osobowych z bazy i ich przekazywania osobom trzecim bez uzasadnienia,
6) użytkownik stanowiska przechowuje wykonaną na nośniku magnetycznym lub optycznym, własną kopię roboczą zaktualizowanych plików (katalogów) pod zamknięciem.

§ 51

Serwisowanie oraz likwidacja nośników i urządzeń wykorzystywanych przy przetwarzaniu danych osobowych

1. Przegląd systemu oraz baz danych odbywa się według rocznego planu przeglądów i konserwacji sporządzonego przez ASI.
2. Sprawdzane są logi systemowe, wykorzystania pojemności dysków i innych zasobów pamięci.
3. Czynności serwisowe systemów informatycznych a w szczególności czynności techniczne istotne dla działania systemu (np. aktualizacja komponentów systemu) wykonywane przez osoby nie zatrudnione w ZTM powinny odbywać się w obecności uprawnionego pracownika ZTM.
4. Nośniki zawierające dane osobowe sprawdzane są w cyklu rocznym pod kątem ich dalszej przydatności.
5. Po stwierdzeniu ich nieprzydatności nośnik zostaje pozbawiony danych lub zniszczony w sposób uniemożliwiający dalszy odczyt informacji przez Komisję powołaną przez ADO.
6. Wszystkie zbiorcze wydruki technologiczne po ich wykorzystaniu podlegają natychmiastowemu zniszczeniu.
7. Urządzenia i nośniki uszkodzone, a zawierające przetwarzane dane osobowe powinny być trwale niszczone o ile pozwalają na to względy finansowe i organizacyjne.
8. Naprawa nośnika danych w specjalistycznym serwisie wymaga podpisania odrębnej umowy lub uzyskania pisemnej gwarancji o niewykorzystywaniu przez serwisanta danych osobowych, bądź też obecności pracownika ZTM przy serwisie.
9. ASI winien dokonywać wybiórczej kontroli kopii, co zostaje potwierdzone protokolarnie.

§ 52

Zabezpieczenie danych osobowych przed utratą spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej, a także przed wystąpieniem siły wyższej

1. Stacje. Na których przetwarzane są dane osobowe winny być zabezpieczone przed awarią zasilania za pomocą urządzenia podtrzymującego zasilenie (UPS). W przypadku pracy na komputerach z wbudowaną baterią (laptop, notebook), zabezpieczenie w urządzenie podtrzymujące (UPS) nie jest wymagane.
2. W przypadku długotrwałych wyłączeń zasilania podstawowego użytkownik powinien wyłączyć stację roboczą.
3. W przypadku wystąpienia siły wyższej zagrażającej danym osobowym, należy zastosować procedurę określoną w załączniku nr 13 do Polityki.

§ 53

Inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania danych osobowych

1. ASI lub wyznaczona przez ADO osoba winna dokonywać inwentaryzacji sprzętu i oprogramowania używanego w ZTM do przetwarzania danych osobowych, co najmniej raz w roku.
2. Wzór dokumentu inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania danych osobowych, stanowi załącznik nr 14 do Polityki.
3. Dopuszczalne jest korzystanie, w zakresie określonym w ust. 1, z systemów informatycznych, które na bieżąco aktualizują i generują raporty zawierające informacje o zainstalowanym sprzęcie informatycznym i oprogramowaniu.

Rozdział VIII
NARUSZENIE OCHRONY DANYCH OSOBOWYCH

§ 54

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik ZTM, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić ADO.
2. W razie niemożliwości zawiadomienia ADO, należy fakt naruszenia zgłosić IOD lub osobie upoważnionej do zastępowania IOD, a jeżeli jest to niemożliwe, należy powiadomić bezpośredniego przełożonego.
3. W przypadku wykrycia naruszenia ochrony danych osobowych, należy postępować zgodnie z procedurą określoną w załączniku nr 15 do Polityki.
4. Jeśli zdarzenie ma charakter przestępstwa sprawa kierowana jest do organów ścigania.

§ 55

Sankcje za naruszenie zasad ochrony danych

1. Nieprzestrzeganie zasad zawartych w dokumentach Polityki, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z Kodeksu pracy i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa.
2. Naruszenie zasad ochrony danych może spowodować pociągnięcie do odpowiedzialności karnej wynikającej z przepisów:
   - RODO oraz innych przepisów normujących kwestie ochrony danych osobowych,
   - Kodeksu karnego, w zakresie przestępstw przeciwko ochronie informacji,
   - chroniących tajemnice służbowe (zawodowe).

Rozdział IX
PRZEPISY PRZEJŚCIOWE

§ 56

Ważność dotychczasowej zgody na przetwarzanie danych osobowych

1. Uzyskane przez ZTM, na podstawie dotychczasowych przepisów, zgody na przetwarzanie danych osobowych, zachowują swoją ważność, z zastrzeżeniem ust. 2
2. W miarę możliwości dotychczasowe zgody, winny być wymieniane lub modyfikowane, tak aby w pełni spełniały wymogi przepisów RODO i Polityki.

Rozdział X
POSTANOWIENIA KOŃCOWE

§ 57

Sposób wypełniania dokumentacji ochrony danych osobowych i dopuszczalne modyfikacje

1. Dokumentacja ochrony danych osobowych w ZTM, w szczególności dokumentacja ujęta w załącznikach do Polityki, stanowi szczegółowe zobrazowanie przyjętego w ZTM systemu ochrony danych osobowych. Dokumentacja ta wina być, zgodnie z przyjętym w Polityce sposobem i terminami, sukcesywnie i dokładnie wypełniana/sprawdzana. Wzory dokumentów, ujęte w załącznikach do Polityki, mogą ulec zmianie, jedynie w drodze zarządzenia Dyrektora ZTM, jako zmiana do Polityki.
2. W przypadku braku lub niepowołania ASI, w rubrykach ich dotyczących stawiamy znak „-„ lub wpisujemy słowo „brak”.
3. W sytuacji, gdy ADO powierzy IOD również zadania ASI, IOD wypełnia lub podpisuje się zarówno w rubrykach odnoszących się do IOD, jak i do ASI.

§ 58

Nakaz współpracy z organem nadzorczym

ADO, procesor oraz ich przedstawiciele mają obowiązek współpracować z UODO na każdym etapie wykonywania przez organ nadzorczy swoich zadań.

§ 59

Nakaz stosowania wszystkich przepisów normujących ochronę danych

1. Uzupełnieniem zapisów Polityki mogą być inne akty wewnętrzne normujące kwestię ochrony danych osobowych, w szczególności odnoszące się do bezpieczeństwa posiadanych i przetwarzanych danych.
2. Do przepisów, o których mowa w ust. 1, można zaliczyć: przepisy BHP i przeciwpożarowe, regulamin korzystania z monitoringu, zasady postępowania z kluczami.
3. W sprawach nieuregulowanych niniejszą Polityką zastosowanie mają wprost przepisy RODO, inne akty wewnętrzne ZTM, w tym wskazane w ust. 2, a także inne przepisy prawa

normujące kwestie szeroko rozumianej ochrony danych, w szczególności przepisy wskazane w § 5 Polityki.

Załącznik nr 1
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

.....
(data nadania upoważnienia)

UPOWAŻNIENIE Nr …./20….
DO PRZETWARZANIA DANYCH OSOBOWYCH

Upoważniam Panią/Pana: ……..
(imię i nazwisko)

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku: ……..
(zajmowane stanowisko, nazwa komórki organizacyjnej)

w zakresie:

…….…….

…….…….

(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba, lub rodzaj czynności/operacji, jakich może dokonywać na danych osobowych)

Identyfikator osoby upoważnionej*:

……

Wystawił:

……...
(podpis administratora/osoby reprezentującej administratora)

Zobowiązuję się do przestrzegania przepisów normujących ochronę danych osobowych, w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) oraz Polityki Ochrony Danych w Zarządzie Transportu Miejskiego w Kielcach.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz informacji o ich zabezpieczeniu, w tym również po ustaniu zatrudnienia.

Przyjął:

…….....
(data i podpis osoby upoważnionej)

* jeżeli dane osobowe przetwarzane są w systemie informatycznym

Załącznik nr 2
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

.....
(data odwołania upoważnienia)

ODWOŁANIE UPOWAŻNIENIA Nr …./20….
DO PRZETWARZANIA DANYCH OSOBOWYCH

Odwołuję z dniem …… upoważnienie do przetwarzania danych osobowych Nr …./20… z dnia ……., wystawione dla Pani/Pana ……..

……...
(podpis administratora/osoby reprezentującej administratora)

Załącznik nr 3
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Zarządzie Transportu Miejskiego w Kielcach

Lp.	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania upoważnienia i podpis ADO/IOD	Data ustania upoważnienia i podpis ADO/IOD	Identyfikator

Załącznik nr 4
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

.....
(data złożenia oświadczenia)

……
(imię i nazwisko)

……..……
(stanowisko pracy lub forma zatrudnienia)

Oświadczenie

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:
   a) Polityki Ochrony Danych w Zarządzie Transportu Miejskiego w Kielcach, w tym o odpowiedzialności karnej za naruszenie ochrony danych osobowych,
   b) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1), tzw. RODO,
   c) o ochronie i postępowaniu z wiadomościami, stanowiącymi tajemnicę służbową,
   d) BHP i przeciwpożarowych.

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałam/ zapoznałem* się z racji wykonywanej pracy w Zarządzie Transportu Miejskiego w Kielcach, a w szczególności nie będę:
   a) ujawniać danych zawartych w eksploatowanych systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   b) ujawniać szczegółów technologicznych używanych systemów oraz oprogramowania,
   c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych zawierających dane osobowe,
   d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującymi ogólnymi przepisami prawa lub przepisami wewnętrznymi, w szczególności Polityką Ochrony Danych w Zarządzie Transportu Miejskiego w Kielcach.

3. Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz informacji o ich zabezpieczeniu, w tym również po ustaniu zatrudnienia.

…….
(podpis)

*niepotrzebne skreślić

Załącznik nr 5
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

Wykaz osób, które zostały zapoznane
z Polityką Ochrony Danych
w Zarządzie Transportu Miejskiego w Kielcach,
a także z RODO i innymi przepisami związanymi z ochroną danych osobowych

Lp.	Nazwisko i imię	Stanowisko	Data	Podpis

Załącznik nr 6
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

Analiza ryzyka w obszarze ochrony danych osobowych

Nazwa aktywu/ zasobu/ systemu	Ryzyko (opis ryzyka, identyfikacja zagrożeń)	Prawdopodobieństwo wystąpienia ryzyka (P)	Skutki wystąpienia ryzyka (S)	P x S	Ocena skutków przetwarzania danych		
					Proponowane działania minimalizujące	Termin realizacji działań minimalizujących	Osoba odpowiedzialna za realizację działań minimalizujących
1	2	3	4	5	6	7	8

1. Wskazanie aktywu/zasobu.
2. Identyfikacja zagrożeń - wskazanie nazwy ryzyka oraz krótki opis ryzyka.
3. Określenie prawdopodobieństwa wystąpienia ryzyka (P):
   - niskie (1) – nie wydarzyło się w ciągu ostatniego roku; nigdy się nie wydarzyło,
   - średnie (2) – zdarza się nieregularnie,
   - wysokie (3) – wydarza się często.
4. Określenie skutków wystąpienia ryzyka (S):
   - niskie (1) – marginalny lub brak wpływu na funkcjonowanie – nie prowadzi do naruszenia przepisów prawa, nie powoduje strat finansowych, wizerunkowych,
   - średnie (2) – ma wpływ na funkcjonowanie - prowadzi do naruszenia przepisów prawa, z wyjątkiem przepisów prawa karnego, powoduje nieznaczne straty finansowe, wizerunkowe,
   - wysokie (3) – ma istotny wpływ na funkcjonowanie – prowadzi do naruszenia przepisów prawa, powoduje znaczne straty finansowe, wizerunkowe.
5. **Poziom ryzyka:**
   - **ryzyko na poziomie wysokim** występuje wtedy, gdy iloczyn prawdopodobieństwa wystąpienia ryzyka (P) i skutku wystąpienia ryzyka (S) będzie większy lub równy 6,
   - **ryzyko na poziomie średnim** występuje wtedy, gdy iloczyn prawdopodobieństwa wystąpienia ryzyka (P) i skutku wystąpienia ryzyka (S) będzie w przedziale 3-4,
   - **ryzyko na poziomie niskim** występuje wtedy, gdy iloczyn prawdopodobieństwa wystąpienia ryzyka (P) i skutku wystąpienia ryzyka (S) będzie w przedziale 1-2.

Ocena skutków:

6. Wskazanie działań minimalizujących (działań naprawczych i sposobów zabezpieczenia danych)
7. Wskazanie terminu realizacji działań minimalizujących.
8. Wskazanie osoby odpowiedzialnej za realizację działań minimalizujących.

Załącznik nr 7
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

Rejestr czynności przetwarzania danych osobowych

Funkcja	Nazwa, Imię i Nazwisko	Dane kontaktowe
Administrator Danych Osobowych		
Inspektor Ochrony Danych		

Lp.	Cel przetwarzania/ Nazwa czynności przetwarzania	Kategoria osób	Kategoria danych	Kategoria odbiorców danych	Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej	Planowany termin usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**

1. Liczba porządkowa czynności przetwarzania.
2. Cel lub nazwa przetwarzania danych osobowych (np. udzielanie informacji publicznej, rekrutacja pracowników).
3. Kategoria osób, których dane dotyczą (np. pracownicy, interesanci).
4. Kategoria danych (konkretny rodzaj danych lub wskazanie: dane zwykłe czy dane wrażliwe, w wersji papierowej czy elektronicznej).
5. Kategoria odbiorców, którym dane osobowe zostały lub zostaną ujawnione.
6. Tak/Nie.
7. Planowane terminy usunięcia poszczególnych kategorii danych. Pomocny w tym zakresie jest Jednolity Rzeczowy Wykaz Akt.
8. Ogólny opis zastosowanych środków bezpieczeństwa – technicznych (fizyczne zabezpieczenia) i organizacyjnych (procedury, wytyczne itp.)

Załącznik nr 8
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

Rejestr kategorii przetwarzania danych przez procesora w imieniu administratora

Funkcja	Nazwa, Imię i Nazwisko	Dane kontaktowe
Podmiot przetwarzający (procesor)		
Administrator Danych Osobowych		
Inspektor Ochrony Danych		

Lp.	Kategoria przetwarzań	Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa
1	**2**	**3**	**4**

1. Liczba porządkowa kategorii przetwarzań.
2. Kategoria przetwarzań dokonywanych w imieniu administratora danych osobowych – ogólna informacja o rodzaju i celu przetwarzania oraz kategorii danych.
3. Tak/Nie.
4. Ogólny opis zastosowanych środków bezpieczeństwa – technicznych (fizyczne zabezpieczenia) i organizacyjnych (procedury, wytyczne itp.).
   W przypadku procesora środkiem bezpieczeństwa o charakterze organizacyjnym może być umowa powierzenia przetwarzania danych osobowych, odpowiednia klauzula w innej umowie merytorycznej lub podpisany przez procesora dokument (oświadczenie) o zapoznaniu się przez procesora z Polityką Ochrony Danych administratora danych osobowych.

Załącznik nr 9
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

Zgoda na przetwarzanie danych osobowych

Oświadczam, że wyrażam zgodę na przetwarzanie moich danych osobowych

……
(imię i nazwisko)

w Zarządzie Transportu Miejskiego w Kielcach
Plac Niepodległości 1
25-001 Kielce
tel. 41 343 15 93
www.ztm.kielce.pl

Jednocześnie przyjmuję do wiadomości, że moje dane osobowe będą wykorzystywane wyłącznie na potrzeby działalności Zarządu Transportu Miejskiego w Kielcach.

Kielce, dnia ……..

…….....
(czytelny podpis)

Klauzula wycofania zgody:
Niniejsza zgoda może zostać wycofana w każdym czasie. W tym celu, należy skontaktować się z Zarządem Transportu Miejskiego, Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93

Podstawa prawna:
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1).

Załącznik nr 10
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Zarząd Transportu Miejskiego w Kielcach, Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, w imieniu którego działa ……. (*imię i nazwisko Dyrektora lub innego prawnego przedstawiciela Zarządu),

2) Administrator powołał inspektora ochrony danych osobowych , z którym można się skontaktować pod adresem iod@ztm.kielce.pl

3) Pani/Pana dane osobowe przetwarzane będą w celu …….. (*należy podać cel przetwarzania), na podstawie ……. (*należy podać podstawę prawną przetwarzania, np. art. 6 ust. 1 lit. a/b/c/d/e/f RODO. *Przy lit. f należy wskazać uzasadniony interes ADO lub strony trzeciej),

4) odbiorcą Pani/Pana danych osobowych będą ……..…….. (*można wymienić kategorię odbiorców o ile istnieją),

5) Pani/Pana dane osobowe będą/nie będą (*niepotrzebne skreślić) przekazywane do państwa trzeciego lub organizacji międzynarodowej, na podstawie (*jeżeli potwierdzone zostało takie przekazywanie - należy wybrać odpowiednią podstawę prawną):

   a) decyzji Komisji Europejskiej, stwierdzającej odpowiedni stopień ochrony …… (*wskazać odpowiednią decyzję),
   b) w tym zakresie nie został stwierdzony przez Komisję Europejską odpowiedni stopień ochrony w drodze decyzji, niemniej dane będą odpowiednio zabezpieczone za pomocą:
      - prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi w postaci ……..…… (*wskazać jakiego),
      - wiążących reguł korporacyjnych …….……. (*wskazać jakich), zatwierdzonych przez UODO,
      - standardowych klauzul ochrony danych przyjętych przez Komisję Europejską - ……..... (*wskazać klauzule),
      - standardowych klauzul ochrony danych przyjętych przez UODO i zatwierdzonych przez Komisję Europejską - ……..... (*wskazać klauzule),
      - zatwierdzonego przez UODO kodeksu postępowania - ..….. (*wskazać jakiego),
      - certyfikatu ochrony danych osobowych - ……..….. (*wskazać jakiego),

- zezwolenia UODO na klauzule umowne - …….. (*klauzule umowne między ADO lub procesorem a ADO, procesorem lub odbiorcą danych w państwie trzecim lub organizacją międzynarodową),
- zezwolenia UODO na postanowienia administracyjne między organami lub podmiotami publicznymi.

Może Pani/Pan uzyskać kopię danych osobowych przekazywanych do państwa trzeciego …….. (*wskazać sposób uzyskania kopii danych lub miejsce udostępnienia danych).

6) Pani/Pana dane osobowe będą przechowywane przez okres …… (*jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu, np. do czasu wyłonienia zwycięzcy konkursu, do czasu zakończenia rekrutacji itp.),

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (*jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem,

8) ma Pani/Pan prawo wniesienia skargi do UODO, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.,

9) podanie przez Panią/Pana danych osobowych jest …… (*wybrać odpowiednio: wymogiem ustawowym/umownym/warunkiem zawarcia umowy). Jest Pani/Pan zobowiązany do ich podania a konsekwencją niepodania danych osobowych będzie ……. (*jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych),

10) Pani/Pana dane będą/nie będą (*niepotrzebne skreślić) przetwarzane w sposób zautomatyzowany, np. w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach ……. (*wskazać jakich), a konsekwencją takiego przetwarzania będzie …….. (*należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą, np. w jaki sposób będą oceniane czynniki osobowe osoby fizycznej, natomiast przykładową konsekwencją takiego przetwarzania mogą być elektroniczne metody rekrutacji bez interwencji ludzkiej).

Załącznik nr 11
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

Wniosek nr …./……
o nadanie uprawnień
do przetwarzania danych osobowych w systemie informatycznym
Zarządu Transportu Miejskiego w Kielcach

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika	**Stanowisko pracy**
Pokój nr:	Telefon nr:
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie	
Użytkownik został zapoznany z przepisami o ochronie danych osobowych.	
Data wniosku:	Podpis przełożonego pracownika:
Podpis IOD:	Podpis ADO i data:
Podpis ASI	

Załącznik nr 12
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

Ewidencja osób upoważnionych
do przetwarzania danych osobowych w systemie informatycznym
Zarządu Transportu Miejskiego w Kielcach

Lp.	Identyfikator użytkownika	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień w systemie	Data i podpis IOD	Data odebrania uprawnień w systemie oraz data i podpis IOD
1.						
	Zmiana danych					
2.						
	Zmiana danych					
3.						
	Zmiana danych					
4.						
	Zmiana danych					

Załącznik nr 13
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

PROCEDURA POSTĘPOWANIA W PRZYPADKU KONIECZNOŚCI WYPROWADZENIA DANYCH OSOBOWYCH POZA STREFĘ OCHRONNĄ Z POWODU WYSTĄPIENIA SIŁY WYŻSZEJ

1. W przypadku wystąpienia siły wyższej (np. zalanie, pożar itp.) należy w zależności od sytuacji:
   1) wyłączyć zawór wodny znajdujący się w budynku,
   2) wyłączyć zasilanie elektryczne urządzenia z danymi w szafce sterowniczej znajdującej się w budynku,
   3) skontaktować się z administratorem budynku pod nr tel. ……., informując o awarii,
   4) wezwać Inspektora Ochrony Danych (tel. ……..),
2. Administrator budynku winien podjąć stosowne kroki, w celu doprowadzenia do usunięcia awarii, czy innego stanu zagrożenia.
3. Inspektor Ochrony Danych, we współpracy z Administratorem Systemu Informatycznego, winien zabezpieczyć urządzenia z danymi oraz po wyznaczeniu miejsca tymczasowego przetrzymywania danych osobowych (suche, bezpieczne pomieszczenie), wynieść zagrożone dane do wskazanego miejsca.
4. Inspektor Ochrony Danych, we współpracy z Administratorem Systemu Informatycznego, winien odtworzyć dane osobowe.

Załącznik nr 14
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

Inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania danych osobowych w Zarządzie Transportu Miejskiego w Kielcach

Lp.	**Nazwa komputera** *(symbol, adres IP, wersja aktualizacji)*	**Główny użytkownik** *(stanowisko pracy, komórka organizacyjna, nr pomieszczenia)*	**Konfiguracja sprzętowa**						**Aplikacje** *(nazwa, wydawca, wersja, ścieżka do pliku)*	**Dane osobowe** *(rodzaje, zbiory)*
			System operacyjny/ BIOS	**Płyta główna**	**Procesor**	**Pamięć**	**Dyski**	**Karty** *(graficzna, dźwiękowa, sieciowa)*		

Załącznik nr 15
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH W ZARZĄDZIE TRANSPORTU MIEJSKIEGO W KIELCACH

§ 1
Cel instrukcji

1. Celem instrukcji jest określenie trybu postepowania w przypadku, gdy:
   1) stwierdzono naruszenie ochrony danych osobowych (działania naprawcze - uruchamiane w przypadku wystąpienia naruszenia danych),
   2) stwierdzono możliwość naruszenia ochrony danych osobowych (czynności profilaktyczne – stosowane w przypadku stwierdzenia, że doszło do incydentu, który nie skutkował naruszeniem ochrony danych).
2. Przykładem zdarzeń, które uruchamiają procedury opisane w niniejszej instrukcji, są m.in.:
   1) stwierdzenie naruszenia zabezpieczenia systemu informatycznego, opisane w § 2,
   2) stwierdzenie, że stan urządzenia, zawartość zbioru danych, ujawnienie metod pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, złamanie zabezpieczeń fizycznych oraz wystąpienie innych zdarzeń, może wskazywać na naruszenie zabezpieczenia danych osobowych. Sytuacje te zostały przykładowo określone w § 3.

§ 2
Naruszenie zabezpieczenia systemu informatycznego

Naruszeniem zabezpieczeń systemu informatycznego jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, uszkodzenie lub zniszczenie danych osobowych lub jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) złamanie kodów dostępu,
2) próba odkodowania zaszyfrowanego dokumentu, pliku,
3) nieautoryzowany dostęp do bazy danych,
4) nieautoryzowane modyfikacje lub niszczenie danych,
5) nielegalne ujawnienie danych,
6) pozyskiwanie danych z nielegalnych źródeł,
7) ujawnienie wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,
8) kradzież sprzętu komputerowego lub nośników zawierających oprogramowanie lub dane,
9) wydarzenia losowe obniżające stan bezpieczeństwa systemu (brak zasilania, pożar, itp.).

§ 3
Sytuacje wskazujące na naruszenie zabezpieczenia danych osobowych

Sytuacjami, które mogą wskazywać, że zostały naruszone zabezpieczenia danych osobowych mogą być takie sytuacje, które odbiegają od przyjętych w ZTM procedur i standardów, a zwłaszcza:

1) naruszenie zasad wynikających z Polityki,
2) naruszenie (uszkodzenie) zabezpieczeń technicznych (fizycznych) w pomieszczeniach (wyłamane zamki, naruszone plomby, ujawnione próby manipulowania przy zamkach itp.), w tym potwierdzone przez organy ściągania dokonanie w ZTM włamania i kradzieży,

3) ujawnienie faktu manipulowania urządzeniami i systemami zabezpieczającymi dostęp do bazy danych,
4) anomalie w pracy systemu lub programu,
5) ujawnienie haseł dostępu do systemu informatycznego,
6) notowanie w krótkim czasie dużej liczby nieudanych prób logowania,
7) korzystanie z zasobów systemu poza zgłoszonymi godzinami pracy,
8) zmiana lub utrata danych zapisanych na kopiach zapasowych lub archiwalnych, dokonana w sposób nieautoryzowany,
9) stwierdzenie nadmiernych, w stosunku do wykonywanych zadań, uprawnień użytkownika do zasobów systemu,
10) nieuprawnione wykonanie kserokopii dokumentu zawierającego dane osobowe,
11) omyłkowe wyniesienie na zewnątrz ZTM dokumentów lub nośników zawierających dane osobowe, przez osobę nieuprawnioną,
12) przesłanie przy użyciu sieci publicznej wiadomości e-mail zawierającej dane osobowe, bez żadnego zabezpieczenia tych danych.

§ 4
Przedmiot instrukcji

Przedmiotem instrukcji są zasady postepowania wszystkich osób zatrudnionych w ZTM, przy przetwarzaniu danych osobowych, a także innych osób uprawnionych do dostępu i/lub przetwarzania danych osobowych w ZTM.

§ 5
Procedura zgłoszenia naruszenia

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego (§ 2 instrukcji) lub gdy zaistniała sytuacja, która mogłaby wskazywać na naruszenie zabezpieczenia danych osobowych (§ 3 instrukcji), każdy pracownik ZTM zatrudniony przy przetwarzaniu danych osobowych lub inna osoba uprawniona do przetwarzania danych osobowych w ZTM, niezwłocznie przerywa przetwarzanie danych osobowych i zawiadamia o tym zdarzeniu ADO.
2. Zgłoszenia faktu naruszenia ochrony danych osobowych należy dokonać niezwłocznie, osobiście lub telefonicznie, a następnie w ciągu 2 godzin od zgłoszenia zaistnienia zdarzenia, określonego w ust. 1, należy opisać powstały incydent wypełniając dokument „Zgłoszenie naruszenia ochrony danych osobowych w Zarządzie Transportu Miejskiego w Kielcach", którego wzór stanowi załącznik nr 1 do niniejszej instrukcji.
3. W przypadku naruszenia, stwierdzonego osobiście przez ADO, spisuje on notatkę służbową, zawierającą wszystkie informacje wskazane we wzorze zgłoszenia, o którym mowa w ust. 2.

§ 6
Podjęcie działań naprawczych

1. ADO, po powzięciu informacji o zdarzeniu, wzywa niezwłocznie ASI i IOD i wraz z nimi podejmuje działania naprawcze, mające na celu:
   1) minimalizację skutków zdarzenia, w tym doprowadzenie do sytuacji uniemożliwiającej dalsze bezprawne przetwarzanie danych osobowych,
   2) zabezpieczenie dowodów zdarzenia,
   3) wyjaśnienie okoliczności zdarzenia,

4) zgłoszenie naruszenia organowi nadzorczemu, zgodnie z § 7 instrukcji,
5) zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, zgodnie z § 8 instrukcji.

2. W celu realizacji zadań wynikających z niniejszej instrukcji ADO, ASI i IOD, lub inna upoważniona przez ADO osoba, ma prawo podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
   1) żądania wyjaśnień od pracowników,
   2) korzystania z pomocy konsultantów,
   3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
3. Polecenia ADO, ASI, IOD lub innej upoważnionej przez ADO osoby, w ramach realizacji zadań wynikających z niniejszej instrukcji, są priorytetowe i winny być wykonane przed innymi.
4. Odmowa udzielenia wyjaśnień lub współpracy z podmiotami wskazanymi w ust. 3 lub z UODO traktowana będzie jako ciężkie naruszenie obowiązków pracowniczych.

§ 7
Zgłoszenie naruszenia organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin od stwierdzenia naruszenia - zgłasza je organowi nadzorczemu, 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. Jeżeli w jakimś zakresie informacji nie da się udzielić niezwłocznie, można je udzielać sukcesywnie bez zbędnej zwłoki.
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
   a) 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 (rekordów) danych osobowych, których dotyczy naruszenie,
   b) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
   d) opisywać środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Wzór zgłoszenia naruszenia ochrony danych osobowych do UODO, stanowi załącznik nr 2 do niniejszej instrukcji.
5. ADO, ze względu na charakter naruszenia lub jeżeli uzna to za stosowne, może dokonać zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, w inny niż wskazany we wzorze sposób, przy spełnieniu wszystkich wymaganych przepisami RODO i niniejszej instrukcji obowiązków w tym zakresie.
6. Podmiot przetwarzający, po stwierdzeniu naruszenia ochrony danych osobowych, oprócz obowiązków, które nakładają na niego przepisy prawa, w tym obowiązku zgłoszenia naruszenia organowi nadzorczemu, również bez zbędnej zwłoki zgłasza ten fakt ADO.

§ 8
Zawiadomienie 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, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1, ma opisywać charakter naruszenia ochrony danych osobowych oraz zawierać informacje i środki, o których mowa w § 7 ust. 2 lit. b, c i d.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   a) gdy, ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   b) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1,
   c) 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.
4. Jeżeli ADO nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy - biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko - może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

§ 9
Zakończenie działań naprawczych

1. IOD lub osoba upoważniona przez ADO po zażegnaniu sytuacji nadzwyczajnej opracowuje raport z przebiegu zdarzenia, w którym powinny się znaleźć:
   1) dane personalne osoby, która stwierdziła naruszenie,
   2) data i godzina zaobserwowania naruszenia,
   3) data i godzina powiadomienia,
   4) rodzaj naruszenia danych osobowych,
   5) opis podjętych czynności i ich uzasadnienie,
   6) potwierdzenie zgłoszenia naruszenia organowi nadzorczemu, lub uzasadnienie braku takiego zgłoszenia,
   7) potwierdzenie zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, lub uzasadnienie braku takiego zawiadomienia.
2. IOD opracowany raport końcowy przedstawia ADO podając w nim przyczyny i skutki zdarzenia oraz wnioski ograniczające możliwość wystąpienia zdarzenia w przyszłości, a także propozycję sankcji dla osób, które spowodowały naruszenie ochrony danych osobowych.

§ 10
Czynności profilaktyczne

1. Jeżeli w wyniku przeprowadzenia procedury zgłoszenia naruszenia ADO stwierdzi, że istniała możliwość naruszenia ochrony danych osobowych, ale do naruszenia nie doszło, ADO, przy udziale IOD i ASI, przeprowadza czynności profilaktyczne, mające za zadanie

zwiększenie zabezpieczenia chronionych i przetwarzanych danych osobowych, polegające m.in. na:

a) wprowadzeniu dodatkowych środków organizacyjnych (np. poprzez wprowadzenie nowej lub uszczegółowienie dotychczasowej Polityki lub innej wewnętrznej procedury),
b) wymianie dotychczasowych (lub wprowadzeniu dodatkowych) zabezpieczeń fizycznych (np. wymiana zamka, założenie kłódki, zamocowanie krat lub rolet antywłamaniowych),
c) wzmocnieniu zabezpieczenia systemu komputerowego (np. zwiększenie częstotliwości zmiany haseł dostępu, zainstalowanie nowszej aplikacji antywirusowej).

2. Opisane w ust. 1 czynności profilaktyczne ADO wdraża również w sytuacji, gdy do naruszenia ochrony danych osobowych doszło, wprowadzono działania naprawcze i całkowicie zniwelowano stan naruszenia i zagrożenia. Czynności te, w tym przypadku, mają służyć zwiększeniu bezpieczeństwa chronionych danych.

§ 11
Rejestr incydentów

1. ZTM dokumentuje wszelkie incydenty i naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania naprawcze i czynności profilaktyczne, w formie Rejestru incydentów, z zastrzeżeniem ust. 2.
2. Nie podlegają udokumentowaniu zgłoszenia oczywiście bezzasadne (np. zgłoszenie naruszenia zamka spowodowanego przez ekipę remontową, dokonującą wymiany drzwi lub zamków w drzwiach, działającą pod nadzorem i na zlecenie ZTM itp.).
3. Rejestr incydentów może posłużyć również UODO, przy wykonywaniu czynności merytorycznych, w tym zaradczych oraz kontrolnych.
4. Rejestr incydentów prowadzi IOD.

§ 12
Sankcje

1. Nie przestrzeganie zasad postepowania określonych w niniejszej instrukcji stanowi ciężkie naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej, wynikającej z Regulaminu pracy, a także określonej w art. 52 i art. 108 Kodeksu Pracy.
2. Jeżeli skutkiem działania określonego w ust. 1 jest ujawnienie informacji osobie nieuprawnionej, sprawca może być pociągnięty do odpowiedzialności karnej wynikającej z Kodeksu Karnego.
3. Jeżeli skutkiem działania określonego w ust. 1 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz prawa cywilnego.

Załącznik nr 1
do Instrukcji postępowania
w sytuacji naruszenia ochrony danych osobowych
w Zarządzie Transportu Miejskiego
w Kielcach

Administrator Danych Osobowych
Zarząd Transportu Miejskiego
w Kielcach
Plac Niepodległości 1
25-001 Kielce

Zgłoszenie naruszenia ochrony danych osobowych
w Zarządzie Transportu Miejskiego w Kielcach

1. Data: ……..…… Godzina: ……
(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

……..
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

……..

……..

……..

……..
(data, podpis osoby zgłaszającej)

Załącznik nr 2
do Instrukcji postępowania
w sytuacji naruszenia ochrony danych osobowych
w Zarządzie Transportu Miejskiego
w Kielcach

……..…….
(miejscowość, data)

.....
(dane adresowe lub pieczęć ADO)

Prezes Urzędu
Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

ZGŁOSZENIE
NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu …..... w ….....

1.	**Charakter naruszenia ochrony danych:**	*Przykładowo:* *przesłanie przez pracownika wiadomości e-mail do błędnego adresata (nieznana osoba) zamiast do współpracownika wraz z załącznikiem w formacie pliku Excel (niezabezpieczonego) zawierającego dane osobowe (takie jak: imię i nazwisko, adres zamieszkania, PESEL, numer telefonu, adresy e-mail).*
2.	**Kategoria i przybliżona liczba osób, których dane dotyczą:**	*Przykładowo:* *Kategoria: interesanci,* *Liczba osób, których dane dotyczą: 20.*
3.	**Liczba rekordów, których dotyczy naruszenie:**	*Przykładowo:* *120*

4.	**Możliwe konsekwencje naruszenia ochrony danych:**	*Przykładowo:* *powstanie szkód majątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub kradzież lub sfałszowanie tożsamości, strata finansowa.*
5.	**Środki zastosowane lub proponowane w celu zaradzeniu naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:**	*Przykładowo:* W*drożenie stosownych środków kryptograficznych, w tym pseudonimizacja, zakaz przesyłania załączników zawierających dane osobowe w sposób niezabezpieczony.*
6.	**Dane inspektora ochrony danych***	*Przykładowo:* *Jan Bezpieczny, nr. telefonu: XXX XXX XXX,* *adres e-mail: iod@domena.pl*

.**
……
……
……...

……
(czytelny podpis administratora danych, zgodnie z reprezentacją podmiotu)

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

Załącznik nr 10
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) dalej zwanym RODO informuję, iż:

administratorem Pani/Pana danych osobowych jest:

1) Zarząd Transportu Miejskiego w Kielcach (zwany dalej: ZTM) z siedzibą Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, e-mail: ztm@ztm.kielce.pl w imieniu którego działa Dyrektor Zarządu Transportu Miejskiego.

2) Administrator powołał inspektora ochrony danych osobowych , z którym można się skontaktować pod adresem iod@ztm.kielce.pl.

3) Pani/Pana dane osobowe przetwarzane będą w celu ochrony mienia oraz zapewnienia bezpieczeństwa pracowników oraz interesantów przebywających w obiektach Zarządu Transportu Miejskiego na podstawie: art. 6 ust. 1 lit. f RODO - prawnie uzasadniony interes administratora, tj. zapewnienie względów bezpieczeństwa, wykorzystanie służy do monitorowania pomieszczeń przed nieautoryzowanym dostępem, co umożliwia przepis art. 222 § 1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy.

4) Monitoring obejmuje:

   a) Pomieszczenia w Punkcie Obsługi Pasażera przy Plac Niepodległości 1,
   b) Korytarze wewnętrzne, klatki schodowe, hole, perony dworca, poczekalnię, drzwi wejściowe, place manewrowe, place postojowe Dworca Autobusowego przy ul. Czarnowskiej 12
   c) Korytarze wewnętrzne, peron dworca, poczekalnię, drzwi wejściowe, mini Dworców Autobusowych przy ul. Jana Nowaka – Jeziorańskiego oraz przy ul. Massalskiego

5) Pani/Pana dane mogą być powierzane i udostępniane następującym podmiotom: uprawnionym do uzyskania danych osobowych na podstawie przepisów prawa (Policja, Prokuratura), świadczącym usługi prawnicze, ochrony mienia, dostawcom systemów informatycznych.

6) Pani/Pana dane osobowe będą przechowywane przez okres do 7 dni od dnia nagrania, a w przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub Administrator powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin powyższy ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

7) Posiada Pani/Pan prawo do żądania od Administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania. Szczegółowe warunki możliwości realizacji ww. praw zawiera RODO. Z wymienionych uprawnień mogą Państwo skorzystać kierując stosowne pismo na adres korespondencyjny lub mailowy na adres Administratora.

8) Mają Państwo prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznają, iż przetwarzanie danych osobowych Państwa dotyczących narusza przepisy RODO.

9) Podanie danych osobowych jest dobrowolne ale niezbędne dla realizacji celów przetwarzania.

10) Państwa dane nie będą przetwarzane w sposób obejmujący zautomatyzowane decyzje, w tym również w formie profilowania.

Załącznik nr 10
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) dalej zwanym RODO informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Zarząd Transportu Miejskiego w Kielcach, Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, e-mail: ztm@ztm.kielce.pl w imieniu którego działa Dyrektor Zarządu Transportu Miejskiego.

2) Administrator powołał inspektora ochrony danych osobowych , z którym można się skontaktować pod adresem iod@ztm.kielce.pl.

3) Pani/Pana dane osobowe przetwarzane będą w celu wykonywania statutowych obowiązków Zarządu Transportu Miejskiego w Kielcach, na podstawie art. 6 ust. 1 lit. e RODO.

4) odbiorcą Pani/Pana danych osobowych będą upoważnienie pracownicy Zarządu Transportu Miejskiego w Kielcach oraz inne podmioty upoważnione na podstawie przepisów prawa,

5) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

6) Pani/Pana dane osobowe będą przechowywane przez okres co najmniej 5 lat co wynika z przepisów archiwizacyjnych i uzależnione jest od rodzaju przechowywanej dokumentacji.

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.

8) ma Pani/Pan prawo wniesienia skargi do UODO, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana narusza przepisy RODO.

9) podanie przez Panią/Pana danych osobowych jest dobrowolne, a konsekwencją niepodania danych osobowych będzie brak możliwości podjęcia czynności statutowych i załatwienia sprawy przez Zarząd Transportu Miejskiego w Kielcach.

10) Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, np. w formie profilowania.

Załącznik nr 10
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) dalej zwanym RODO informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Zarząd Transportu Miejskiego w Kielcach, Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, e-mail: ztm@ztm.kielce.pl w imieniu którego działa Dyrektor Zarządu Transportu Miejskiego.

2) Administrator powołał inspektora ochrony danych osobowych , z którym można się skontaktować pod adresem iod@ztm.kielce.pl.

3) Pani/Pana dane osobowe przetwarzane będą w celu i w zakresie niezbędnym dla potrzeb pobrania opłaty dodatkowej na podstawie art.6 ust. 1 lit e) RODO oraz innych obowiązujących przepisów prawa w szczególności z dnia 15.11.1984r. Prawo przewozowe (t.j. Dz.U.2020.8)

4) odbiorcą Pani/Pana danych osobowych będą upoważnienie pracownicy Zarządu Transportu Miejskiego w Kielcach, podmioty świadczące usługi prawnicze, archiwiści, podmioty świadczące usługi IT oraz inne podmioty upoważnione na podstawie przepisów prawa,

5) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

6) Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do dochodzenia opłaty dodatkowej, a po jej uiszczeniu przez czas wykonywania obowiązków wynikających z przepisów prawa.

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.

8) ma Pani/Pan prawo wniesienia skargi do UODO, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana narusza przepisy RODO.

9) podanie przez Panią/Pana danych osobowych jest obowiązkowe i wynika z ustawy Prawo przewozowe, a w razie odmowy ich podania osoba upoważniona przez organizatora publicznego transportu zbiorowego ma prawo ująć podróżnego i niezwłocznie oddać go w ręce Policji lub innych organów porządkowych, które mają

zgodnie z przepisami prawo zatrzymania podróżnego i podjęcia czynności zmierzających do ustalenia jego tożsamości.

10) Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, np. w formie profilowania.

Załącznik nr 10
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) dalej zwanym RODO informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Zarząd Transportu Miejskiego w Kielcach, Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, e-mail: ztm@ztm.kielce.pl w imieniu którego działa Dyrektor Zarządu Transportu Miejskiego.

2) Administrator powołał inspektora ochrony danych osobowych , z którym można się skontaktować pod adresem iod@ztm.kielce.pl.

3) Pani/Pana dane osobowe przetwarzane będą w celu zawarcia umowy o pracę na podstawie art. 6 ust. 1 lit. b RODO. W razie konieczności dane mogą być udostępniane podmiotom udzielającym świadczeń zdrowotnych, podmiotowi organizującemu szkolenia w zakresie bhp, zakładom ubezpieczeń i brokerom ubezpieczeniowym.

4) odbiorcą Pani/Pana danych osobowych będą upoważnienie pracownicy Zarządu Transportu Miejskiego w Kielcach oraz inne podmioty upoważnione na podstawie przepisów prawa,

5) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

6) Pani/Pana dane osobowe będą przechowywane przez okres co najmniej 50 lat, co wynika z przepisów archiwizacyjnych i uzależnione jest od rodzaju przechowywanej dokumentacji.

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.

8) ma Pani/Pan prawo wniesienia skargi do UODO, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana narusza przepisy RODO.

9) podanie przez Panią/Pana danych osobowych jest dobrowolne, a konsekwencją niepodania danych osobowych będzie brak możliwości podjęcia czynności statutowych i załatwienia sprawy przez Zarząd Transportu Miejskiego w Kielcach.

10) Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, np. w formie profilowania.

Załącznik nr 10
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

1. administratorem Pani/Pana danych osobowych jest Zarząd Transportu Miejskiego w Kielcach, Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, e-mail: ztm@ztm.kielce.pl w imieniu którego działa Dyrektor Zarządu Transportu Miejskiego.

2. Administrator powołał inspektora ochrony danych osobowych , z którym można się skontaktować pod adresem iod@ztm.kielce.pl.

3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego;

4. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy Prawo zamówień publicznych (Dz.U. z dnia 24.10.2019, poz. 2019 z późniejszymi zmianami);

5. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia lub na okres przechowywania tych danych zgodnie z wytycznymi o dofinansowania z środków UE;

6. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

7. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;

8. posiada Pani/Pan:

   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych*;
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO **;

- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9. nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.
- Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego.
- W trakcie oraz po zakończeniu postępowania o udzielenie zamówienia publicznego, w przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 rozporządzenia 2016/679, wymagałoby niewspółmiernie dużego wysiłku, zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających w szczególności na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.

* Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.

** Wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

Załącznik nr 10
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) dalej zwanym RODO informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Zarząd Transportu Miejskiego w Kielcach, Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, e-mail: ztm@ztm.kielce.pl w imieniu którego działa Dyrektor Zarządu Transportu Miejskiego.

2) Administrator powołał inspektora ochrony danych osobowych , z którym można się skontaktować pod adresem iod@ztm.kielce.pl.

3) Pani/Pana dane osobowe przetwarzane będą w celu zawarcia umowy o pracę na podstawie art. 6 ust. 1 lit. b RODO. W razie konieczności dane mogą być udostępniane podmiotom udzielającym świadczeń zdrowotnych, podmiotowi organizującemu szkolenia w zakresie bhp, zakładom ubezpieczeń i brokerom ubezpieczeniowym.

4) odbiorcą Pani/Pana danych osobowych będą upoważnienie pracownicy Zarządu Transportu Miejskiego w Kielcach oraz inne podmioty upoważnione na podstawie przepisów prawa,

5) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

6) Pani/Pana dane osobowe będą przechowywane do momentu zakończenia procesu rekrutacyjnego.

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.

8) ma Pani/Pan prawo wniesienia skargi do UODO, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana narusza przepisy RODO.

9) podanie przez Panią/Pana danych osobowych jest dobrowolne, a konsekwencją niepodania danych osobowych będzie brak możliwości podjęcia czynności statutowych i załatwienia sprawy przez Zarząd Transportu Miejskiego w Kielcach.

10) Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, np. w formie profilowania.

Załącznik nr 10
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) dalej zwanym RODO informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Zarząd Transportu Miejskiego w Kielcach, Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, e-mail: ztm@ztm.kielce.pl w imieniu którego działa Dyrektor Zarządu Transportu Miejskiego.

2) Administrator powołał inspektora ochrony danych osobowych , z którym można się skontaktować pod adresem iod@ztm.kielce.pl.

3) Pani/Pana dane osobowe przetwarzane będą w celu zgłoszenia i likwidacji szkody na podstawie art. 6 ust. 1 lit. a RODO. Podanie danych jest dobrowolne ale niezbędne w celu likwidacji szkody.

4) odbiorcą Pani/Pana danych osobowych będą upoważnienie pracownicy Zarządu Transportu Miejskiego w Kielcach oraz inne podmioty upoważnione na podstawie przepisów prawa, w tym podmioty świadczące usługi ubezpieczeniowe dla Administratora.

5) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

6) Pani/Pana dane osobowe będą przechowywane przez okres co najmniej 5 lat co wynika z przepisów archiwizacyjnych i uzależnione jest od rodzaju przechowywanej dokumentacji.

7) posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.

8) ma Pani/Pan prawo wniesienia skargi do UODO, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana narusza przepisy RODO.

9) podanie przez Panią/Pana danych osobowych jest dobrowolne, a konsekwencją niepodania danych osobowych będzie brak możliwości podjęcia czynności statutowych i załatwienia sprawy przez Zarząd Transportu Miejskiego w Kielcach.

10) Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, np. w formie profilowania.

Załącznik nr 10
do Polityki Ochrony Danych
w Zarządzie Transportu Miejskiego
w Kielcach

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) dalej zwanym RODO informuję, iż:

administratorem Pani/Pana danych osobowych jest:

1) Zarząd Transportu Miejskiego w Kielcach (zwany dalej: ZTM) z siedzibą ul. Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, e-mail: ztm@ztm.kielce.pl w imieniu którego działa Dyrektor Zarządu Transportu Miejskiego.

2) Miejskie Przedsiębiorstwo Komunikacji w Kielcach Sp. z o.o. (zwany dalej MPK) z siedzibą: ul. Jagiellońska 92, 25-734 Kielce; – będących współadministratorami danych w zakresie niezbędnym dla realizacji publicznego transportu zbiorowego, wspólnie na podstawie umowy zawartej w dniu 24.05.2018 o współadministrowanie danymi osobowymi.

3) Kontakt do inspektora ochrony danych osobowych ZTM: e-mail: iod@ztm.kielce.pl. Kontakt do MPK iod@mpk.kielce.pl

4) Współadministratorzy będą przetwarzać dane celem badania potoków pasażerskich, wyjaśnienia sytuacji konfliktowych związanych z wniesionymi skargami, odwołaniami, reklamacjami, ustalenia sprawców czynów nagannych lub zabronionych, lub w dowolnym celu będącym realizacją prawnie uzasadnionego interesu zabezpieczenia informacji na wypadek potrzeby wykazania faktów lub obrony przed ewentualnymi, roszczeniami na podstawie przepisów prawa, w tym w szczególności prawa przewozowego na podstawie: art. 6 ust. 1 lit. d) i f) RODO.

5) Państwa dane mogą być powierzane i udostępniane następującym podmiotom: uprawnionym do uzyskania danych osobowych na podstawie przepisów prawa (Policja, Prokuratura), świadczącym usługi prawnicze, ochrony mienia, dostawcom systemów informatycznych.

6) Państwa dane osobowe będą przechowywane przez okres do 7 dni od dnia nagrania, a w przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub Administratorzy powzięli wiadomość, iż mogą one stanowić dowód w postępowaniu, termin powyższy ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

7) Posiadają Państwo prawo do żądania od Administratorów dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania. Szczegółowe warunki możliwości realizacji ww. praw zawiera RODO. Z wymienionych uprawnień mogą Państwo

skorzystać kierując stosowne pismo na adres korespondencyjny lub mailowy jednego ze Współadministratorów wskazany odpowiednio w pkt 1) lub 2).

8) Mają Państwo prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznają, iż przetwarzanie danych osobowych Państwa dotyczących narusza przepisy RODO.

9) Podanie danych osobowych jest dobrowolne ale niezbędne dla realizacji celów przetwarzania.

10) Państwa dane nie będą przetwarzane w sposób obejmujący zautomatyzowane decyzje, w tym również w formie profilowania.

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych osobowych) dalej zwanym RODO informuję, iż:

administratorem Pani/Pana danych osobowych jest:

1) Zarząd Transportu Miejskiego w Kielcach (zwany dalej: ZTM) z siedzibą Plac Niepodległości 1, 25-001 Kielce, tel. 41 343 15 93, e-mail: ztm@ztm.kielce.pl w imieniu którego działa Dyrektor Zarządu Transportu Miejskiego.

2) Miejskie Przedsiębiorstwo Komunikacji w Kielcach Sp. z o.o. (zwany dalej MPK) z siedzibą: ul. Jagiellońska 92, 25-734 Kielce; – będących współadministratorami danych w zakresie niezbędnym dla realizacji publicznego transportu zbiorowego, wspólnie na podstawie umowy zawartej w dniu 24.05.2018r. o współadministrowanie danymi osobowymi.

3) Kontakt do inspektora ochrony danych osobowych ZTM: e-mail: iod@ztm.kielce.pl. Kontakt do MPK iod@mpk.kielce.pl

4) Współadministratorzy będą przetwarzać dane celem badania potoków pasażerskich, wyjaśnienia sytuacji konfliktowych związanych z wniesionymi skargami, odwołaniami, reklamacjami, ustalenia sprawców czynów nagannych lub zabronionych, lub w dowolnym celu będącym realizacją prawnie uzasadnionego interesu zabezpieczenia informacji na wypadek potrzeby wykazania faktów lub obrony przed ewentualnymi, roszczeniami na podstawie przepisów prawa, w tym w szczególności prawa przewozowego na podstawie: art. 6 ust. 1 lit. d) i f) RODO.

5) Pełna klauzula informacyjna dostępna jest pod adresem : www.ztm.kielce.pl/.../....