Załącznik do Uchwały Nr 70/VII/2021
z dnia 27.07.2021r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W MIĘDZYGMINNYM ZWIĄZKU KOMUNIKACYJNYM W JASTRZĘBIU ZDROJU.

1. POSTANOWIENIA OGÓLNE

Niniejsza instrukcja reguluje w szczególności sposób zarządzania systemem informatycznym w Międzygminnym Związku Komunikacyjnym w Jastrzębiu Zdroju, służącym do przetwarzania danych osobowych z uwzględnieniem wymogów określonych w § 5 rozporządzenia ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100 poz.1024) stanowiący merytoryczną podstawę do wyznaczenia standardów w tym zakresie.

2. DEFINICJE POJĘĆ UŻYTYCH W INSTRUKCJI ORAZ WYKAZ APLIKACJI PROGRAMOWYCH I ZAKRES PRZETWARZANIA DANYCH.

2.1. DEFINICJE:

Danymi osobowymi – jest każda informacja o zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Systemem informatycznym – jest zespół współpracujących ze sobą urządzeń, oprogramowania, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

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

W przypadku niniejszej Polityki Administratorem jest: Międzygminny Związek Komunikacyjny w Jastrzębiu Zdroju, 44-335 Jastrzębie-Zdrój, ul. Przemysłowa 1.

Inspektorem Ochrony Danych Osobowych bądź IODO jest osoba wyznaczona przez Zarząd MZK do realizacji obowiązków w zakresie całokształtu spraw wynikających z przepisów powszechnie obowiązujących oraz procedur wewnętrznych, a dotyczących przetwarzania danych osobowych.

Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany bądź nie zautomatyzowany np.: zbieranie, utrwalanie, organizowanie, porządkowanie,

przechowywanie, adaptowanie lub rozpowszechnianie lub inne udostępnianie, łączenie, ograniczenie, usuwanie bądź niszczenie.

Administratorem systemu informatycznego jest osoba wyznaczona przez Zarząd MZK odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych.

Użytkownikiem jest osoba posiadająca polecenie wydane przez *administratora* w zakresie w nim wskazanym do przetwarzania danych osobowych w systemie informatycznym, która posiada indywidualny identyfikator oraz hasło lub posiada polecenie do przetwarzania danych osobowych w formie tradycyjnej.

2.2. WYKAZ APLIKACJI PROGRAMOWYCH I ZAKRES DANYCH PRZETWARZANYCH.

M Z K w Jastrzębiu Zdroju korzysta z następujących aplikacji, w których przetwarza się dane osobowe:

a/ **Informatyczny System Obsługi i Bezpieczeństwa Pasażerów**
Jest to system obejmujący:
- elektroniczną sprzedaż tzw. e-biletów,
- tablice informacyjne e-rozkładów jazdy,
- zarządzanie ruchem i geolokalizacją autobusów,
- system monitoringu w autobusach,
- portal użytkownika karty e-biletu,

b/ **Windykator 2**
Rejestracja dłużników, rejestracja mandatów, rejestracja wpłat za mandaty, prowadzenie spraw sądowych i komorniczych, rozliczanie prowizji.
c/ **Pakiet Ratusz** - księgowość, środki trwałe,
d/ **system Kadry i Płace – Rekord** - prowadzenie spraw kadrowo-płacowych
e/ **e-Dokument** – **Rekord** - System zarządzania dokumentacją w Biurze MZK,
f/ **Dostęp do rejestru PESEL (MSWiA).**

2.3. W zbiorze danych osobowych przetwarzanych w MZK są dane osobowe:
2.3.1. osób zatrudnionych w MZK według zakresu określonego art. 22^1 ustawy kodeks pracy
2.3.2. osób-kandydatów do pracy zgodnie z zakresem art. 22^1 ustawy kodeks pracy
2.3.3. osób użytkowników karty e-bilet,
2.3.4. osób użytkowników karty jastrzębianina,
2.3.5. osób użytkowników serwisu smsowego związanego z powiadomieniami,
2.3.6. osób pasażerów autobusów realizujących transport miejski w zakresie monitoringu stosowanego w tych pojazdach,
2.3.7. kontrahentów MZK, którzy mają podpisaną umowę cywilną na dostawę towarów, bądź świadczenie usług,
2.3.8. osób fizycznych związanych umową cywilną z MZK,

2.3.9. osób fizycznych dłużników.

3. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALEJ ZA TE CZYNNOŚCI.

3.1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca polecenie do przetwarzania danych osobowych.

3.2. IODO jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

3.3. Osobą odpowiedzialną za rejestrację uprawnień użytkowników w systemach informatycznych jest administrator systemu informatycznego.

3.4. Procedura nadawania, cofania oraz modyfikacji uprawnień do przetwarzania danych osobowych:
3.4.1. Polecenie, o którym mowa w punkcie 3.1 zostaje wydane użytkownikowi na wniosek pracownika MZK. Polecenie zostaje wystawione przez IODO i podlega zatwierdzeniu przez ADO
3.4.2. Wniosek winien zawierać dokładny opis uprawnień, które powinny zostać nadane, cofnięte lub zmodyfikowane, oraz okres przez jaki uprawnienia powinny obowiązywać. Wzór wniosku stanowi załącznik nr 1 do instrukcji.
3.4.3. Jeżeli polecenie dotyczy przetwarzania danych w systemie informatycznym, po jego udzieleniu przez *Administratora*, IODO przekazuje informację wynikającą z upoważnienia administratorowi systemu informatycznego, który realizuje uprawnienia użytkownika w systemie informatycznym.
3.4.4. IODO prowadzi ewidencję osób upoważnionych do przetwarzania danych zawierającą w szczególności: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia, identyfikator – jeżeli dane są przetwarzane w systemie informatycznym.

3.5. Ustanie stosunku pracy jest równoznaczne z wygaśnięciem uprawnień do przetwarzania danych osobowych.

3.6. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

3.7. IODO oraz administrator systemu informatycznego są jednocześnie użytkownikami uprzywilejowanymi.

4. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.

4.1. Dane osobowe przetwarzane są w MZK z użyciem dedykowanych serwerów, komputerów stacjonarnych i przenośnych, pamięci zewnętrznych.

4.2. Administrator systemu informatycznego przydziela użytkownikowi hasło. Przydział hasła użytkownikowi następuje bezzwłocznie. Hasło zostaje przekazane użytkownikowi w formie ustnej. Hasło to użytkownik zobowiązany jest zmienić po pierwszym uwierzytelnieniu się w systemie oraz w okresie późniejszym nie rzadziej niż co 90 dni.

4.3. Hasło powinno składać się z co najmniej 8 znaków zawierających małe i wielkie litery oraz cyfry lub znaki specjalne. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej. Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika takie jak: nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej.

4.4. Ustanie stosunku pracy powoduje wygaśnięcie upoważnienia do przetwarzania danych oraz wyrejestrowanie użytkownika jeżeli posiadał on upoważnienie do przetwarzania danych w systemie informatycznym. Identyfikator po wyrejestrowaniu użytkownika nie może być przydzielony innej osobie.

4.5. W przypadku, gdy istnieje uzasadnione podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie administratora systemu informatycznego bądź IODO

5. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU.

5.1. W celu rozpoczęcia pracy w systemie informatycznym użytkownik obowiązany jest do podania identyfikatora oraz hasła dostępu do systemu. W przypadku pierwszego uwierzytelniania się w systemie użytkownik ma obowiązek zmiany hasła. Zabrania się wpisywania hasła lub jego zmiany w obecności innych osób.
W przypadku gdy użytkownik zapomni hasła, musi skontaktować się z administratorem systemu informatycznego w celu uzyskania nowego hasła.

5.2. W celu zawieszenia pracy w systemie informatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest do wyrejestrowania się z systemu. Wznowienie pracy z systemem wymaga zastosowania się do procedury zawartej w pkt. 5.1. Zabrania się pozostawiania stanowiska komputerowego z uruchomionym systemem bez kontroli pracującego na nim użytkownika.

5.3. Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu poprzez uruchomienie odpowiedniej dla danego systemu operacyjnego opcji jego zamknięcia. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji zamknięcia systemu.

5.4. Użytkownik powinien bezzwłocznie powiadomić administratora systemu informatycznego bądź IODO w przypadku braku możliwości zalogowania się na swoje konto w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. IODO wszczyna postępowanie wyjaśniające i jeżeli stwierdzi faktyczne naruszenie zabezpieczeń sytemu informatycznego rejestruje to jako incydent. Weryfikowane jest czy stanowi to naruszenie, które rodzi powstanie zawiadomienia osób, której dane dotyczą lub organowi nadzorczemu.

6. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.

6.1. Urządzenia służące do przetwarzania danych osobowych (serwery, komputery stacjonarne) muszą być zabezpieczone przed awarią zasilania i zakłóceniami w sieci zasilającej za pomocą urządzeń zabezpieczających (zasilacze awaryjne).

6.2. Kopie zapasowe na urządzeniach informatycznych tworzone są raz w tygodniu. Administrator systemu informatycznego okresowo sprawdza wykonane kopie pod kątem ich poprawności i przydatności do wykorzystania w przypadku awarii systemu.

6.3. W szczególnych przypadkach, np. przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu. Kopię tą wykonuje administrator systemu informatycznego.

6.4. Urządzenia, dyski lub inne nośniki informatyczne zawierające dane osobowe, przeznaczone do likwidacji muszą być pozbawione zapisu tych danych lub uszkodzone w sposób uniemożliwiający ich odczytanie.

7. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH.

7.1. Dostęp do nośników z kopiami zapasowymi systemu ma wyłącznie IODO oraz administrator systemu informatycznego.

7.2. Wszelkie wydruki zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub

pomieszczeniach i po upływie czasu ich przydatności są niszczone przy użyciu niszczarek dokumentów lub przekazywane do zniszczenia wyspecjalizowanej firmie.

7.3. Kopie zapasowe systemu, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych, a w przypadku gdy nie jest to możliwe, niszczy w stopniu uniemożliwiającym ich odczytanie.

8. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁANIEM OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.

8.1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych ze strony wirusów komputerowych oraz innego złośliwego oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych. Wirusy komputerowe oraz wyżej wymienione oprogramowanie mogą pojawić się w systemach MZK poprzez: sieć internetową, nośniki informacji takie jak: płyty CD, DVD, dyski przenośne, pamięci typu flash, pocztę elektroniczną itp.

8.2. W celu zabezpieczenia systemu informatycznego przed zagrożeniami, o których mowa w pkt. 8.1 MZK wykorzystuje oprogramowanie antywirusowe, zainstalowane na każdym stanowisku komputerowym, które posiada dostęp do Internetu. Aktualizacja oprogramowania antywirusowego jest automatyczna. Do obowiązków administratora systemu informatycznego należy okresowa weryfikacja stanu oprogramowania antywirusowego oraz jego aktualności.

8.3. Sieć komputerowa jest zabezpieczona przed nieautoryzowanym dostępem z zewnątrz poprzez oprogramowanie typu *firewall*, zainstalowane na komputerze pełniącym funkcję bramy dostępowej do Internetu. Dodatkowo *firewall* musi być uaktywniony na każdym stanowisku komputerowym posiadającym dostęp do sieci Internet.

8.4. Elektroniczne nośniki informacji takie jak dyski przenośnie, pamięci typu *flash* itp. należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do administratora systemu informatycznego.

8.5. W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z IODO bądź administratorem systemu informatycznego.

8.6. Zezwala się jedynie na korzystanie z poczty elektronicznej służbowej. Przy korzystaniu z poczty elektronicznej służbowej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od nieznanych nadawców.

8.7. Zabrania się użytkownikom komputerów wyłączania, blokowania oraz odinstalowywania programów zabezpieczających komputer przed złośliwym oprogramowaniem oraz nieautoryzowanym dostępem.

9. UDOSTĘPNIANIE DANYCH OSOBOWYCH I SPOSÓB ODNOTOWANIA INFORMACJI O UDOSTĘPNIONYCH DANYCH.

9.1. Udostępnianie danych osobowych instytucjom lub osobom spoza MZK zachodzi w przypadkach określonych przepisami prawa. Zgodę na udostępnienie danych osobowych opiniuje IODO, a wydaje wyłącznie Administrator po analizie zasadności wniosku.

10. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.

10.1. Przeglądy (dokonywane również według kryterium legalności oprogramowania zainstalowanego na poszczególnych stanowiskach komputerowych) i konserwacje systemów oraz nośników informacji wykonuje administrator systemu informatycznego w celu zapewnienia bezpieczeństwa i ciągłości pracy w zakresie przetwarzanych danych nie rzadziej niż raz w roku.

10.2. Naprawa sprzętu, na którym mogą znajdować się dane osobowe, wykonywana przez pracowników firm zewnętrznych, powinna odbywać się pod nadzorem administratora systemu informatycznego w miejscu jego użytkowania.

10.3. W przypadku konieczności naprawy sprzętu, na którym mogą znajdować się dane osobowe poza miejscem użytkowania, dane te należy zarchiwizować na nośniki informacji, a dyski twarde bezwzględnie wymontować na czas naprawy. W przypadku braku możliwości wymontowania, dane na dyskach twardych powinny być usunięte | w sposób uniemożliwiający ich odtworzenie. Za czynności te odpowiada administrator systemu informatycznego.

10.4 Przed likwidacją sprzętu, w którym znajdują się dane osobowe, administrator systemu informatycznego wymontowuje wszystkie dyski twarde oraz usuwa dane zapisane na tych dyskach lub uszkadza je w sposób uniemożliwiający ich odczytanie.

10.5. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora systemu informatycznego.

11. USTALENIA KOŃCOWE.

11.1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe zabrania się:
11.1.1. ujawniania hasła współpracownikom i osobom z zewnątrz,
11.1.2. udostępniania osobom nieupoważnionym programów komputerowych zainstalowanych w systemie,
11.1.3. kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza MZK,
11.1.4. samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego, programy komputerowe instalowane są wyłącznie przez administratora systemu informatycznego,
11.1.5. używania nośników danych udostępnionych przez osoby postronne,
11.1.6. przysyłania oraz odbierania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (nie służbowego),
11.1.7. narażenia sprzętu i nośników danych na kradzież (np. poprzez pozostawienie komputera przenośnego w miejscu publicznym np. w samochodzie itp.),
11.1.8 pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach, w których przetwarzane są dane osobowe.

11.2. Wszelkie przypadki naruszenia niniejszej instrukcji należy zgłaszać IODO.

11.3. IODO prowadzi ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązały się do przestrzegania zasad w nim zawartych.

11.4 IODO przyjmuje od pracownika oświadczenie według wzoru stanowiącego załącznik nr 2. Kadry przechowują oświadczenie i polecenie do przetwarzania danych osobowych.

Jastrzębie Zdrój, ...
data

Załącznik nr 1

Dla pracowników

Polecenie do przetwarzania danych osobowych w M Z K Jastrzębie-Zdrój

Na podstawie art. 29 w związku z art. 32 ust.4 ***rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1)*** – dalej zwane **RODO** niniejszym Administrator który ustala cele i sposoby przetwarzania danych osobowych w M Z K z siedzibą w Jastrzębiu-Zdroju przy ulicy Przemysłowej 1, poleca i upoważnia do przetwarzania danych osobowych:

Panią/~~Pana~~ _____stanowisko _____

w następującym zakresie:

_____

Polecenie to obowiązuje w czasie wykonywania pracy na powyższym stanowisku pracy.

....

INSPEKTOR OCHRONY DANYCH OSOBOWYCH ADMINISTRATOR DANYCH OSOBOWYCH

Załącznik nr 2

Jastrzębie Zdrój, ……..

…… data

……

dane pracownika
Imię i nazwisko i adres zamieszkania

OŚWIADCZENIE

Oświadczam, że zapoznałam /em/ się na przeprowadzonym szkoleniu z przepisami dotyczącymi ochrony danych osobowych oraz przyjętą do stosowania dokumentacją bezpieczeństwa stosowaną w Międzygminnym Związku Komunikacyjnym z siedzibą przy ulicy Przemysłowej w Jastrzębiu-Zdroju. Jednocześnie zobowiązuje się do:
- zachowania w tajemnicy, także po ustaniu stosunku pracy, przetwarzanych przeze mnie danych osobowych oraz sposobów ich ochrony,
- do zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem

……
Podpis upoważnionego

Szkolenie zostało przeprowadzone przez IODO zarejestrowanego w Ogólnokrajowym Rejestrze IODO prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych w Warszawie.

Potwierdzenie przeprowadzenia szkolenia ……
data i czytelny podpis Inspektora Ochrony Danych Osobowych