UCHWAŁA NR 32/2016
ZARZĄDU ZWIĄZKU MIAST I GMIN POJEZIERZA DRAWSKIEGO
z dnia 31 sierpnia 2016 r.

w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) oraz § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w spawie 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), zarządza się, co następuje:

§ 1.1. Wprowadza się dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Związku Miast i Gmin Pojezierza Drawskiego.

2. Na dokumentację, o której mowa w ust. 1 składa się:

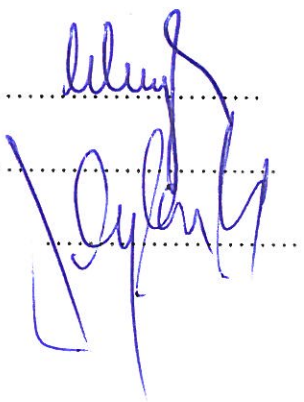
a) Polityka bezpieczeństwa zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiąca załącznik nr 1 do uchwały,

b) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Związku Mast i Gmin Pojezierza Drawskiego, stanowiąca załącznik nr 2 zarządzenia.

§2. Uchwała wchodzi w życie z dniem podjęcia.

Zarząd Związku Miast i Gmin Pojezierza Drawskiego:

1. Przewodniczący Zarządu – Waldemar Włodarczyk .....
2. Zastępca Przewodniczącego Zarządu – Piotr Ćwikła .....
3. Członek Zarządu – Stanisław Cybula .....



Zatwierdzam pod względem formalno-prawnym
RADCA PRAWNY
Katarzyna Potocka

Załącznik nr 1
do Uchwały Nr 32/2016
Zarządu Związku Miast i Gmin Pojezierza Drawskiego
z dnia 31 sierpnia 2016r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH ZWIĄZKU MIAST I GMIN POJEZIERZA DRAWSKIEGO

-2016-

Spis treści

Wykaz załączników

1. Wprowadzenie

Polityka bezpieczeństwa danych osobowych opisuje środki techniczne i organizacyjne zapewniające ochronę podczas przechowywania i przetwarzania danych osobowych (w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych Dz. U. z 2015r. poz. 2135 z późn. zm.) w Związku Miast i Gmin Pojezierza Drawskiego.

Podstawa prawna dokumentu

- Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2015r. poz. 2135 z pózn. zm.).
- Rozporządzenie 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).

2. Definicje

a) Związek – w niniejszym dokumencie oznacza Związek Miast i Gmin Pojezierza Drawskiego,

b) Administrator Danych Osobowych (ADO) - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. Funkcję ADO w Związku pełni Zarząd Związku Miast i Gmin Pojezierza Drawskiego, zwany dalej zarządem Związku,

c) Administrator Bezpieczeństwa Informacji (ABI) – pracownik Związku, wyznaczony przez ADO do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych. Funkcję ABI w Związku pełni osoba wyznaczona przez Zarząd Związku,

d) Administrator Systemu Informatycznego (ASI) - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w Związku

e) Użytkownik systemu – osoba, która została upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być pracownik Związku, jak również osoba odbywająca staż lub praktykę w Związku.

f) System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

g) Dane osobowe – informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

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

i) Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, w tym zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

j) Sieć lokalna (Local Area Network) – połączenie komputerów pracujących w Związku w celu wymiany danych dla potrzeb wewnętrznych, przy wykorzystaniu urządzeń sieciowych.

k) Hasło – jest to ciąg znaków znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

l) Identyfikator (Id) – ciąg znaków jednoznacznie identyfikujący użytkownika.

m) Ustawa o ochronie danych osobowych - ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 z późn. zm.)

3. Obowiązki Administratora Bezpieczeństwa Informacji

a) Nadzór nad przestrzeganiem zasad ochrony danych osobowych.

b) Udzielanie informacji osobom, których dane są zbierane (art. 24 i 25 ustawy o ochronie danych osobowych).

c) Udzielanie, na wniosek osoby, której dane dotyczą, informacji o zakresie przetwarzanych danych osobowych (art. 33 ust. o ochronie danych osobowych).

d) Obowiązek uzupełniania, uaktualnienia, sprostowania, wstrzymania przetwarzania danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane (art. 35 ust. o ochronie danych osobowych).

e) Zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38 ust. o ochronie danych osobowych).

f) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych - załącznik nr 1 (art. 39 ust. o ochronie danych osobowych).

g) Zgłaszanie zbiorów do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (art. 40 ust. o ochronie danych osobowych).

h) Zabezpieczeniem danych przed ich udostępnieniem osobom nieupoważnionym.

i) Nadzór nad obiegiem, przechowywaniem oraz usuwaniem danych osobowych.

j) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń, na których zapisane są dane osobowe.

k) Przeciwdziałanie przetwarzaniu danych z naruszeniem ustawy o ochronie danych osobowych.

l) Monitorowanie zabezpieczeń stosowanych w celu ochrony danych osobowych.

m) Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, lub podejrzenia naruszenia zabezpieczeń.

4. Obszar przechowywania i przetwarzania danych osobowych wraz z wykazem zbiorów danych osobowych oraz ze wskazaniem programów zastosowanych do ich przetwarzania

Dane osobowe przechowywane i przetwarzane są w wyznaczonych pomieszczeniach budynku, w którym mieści się Związek. Wykaz pomieszczeń wraz ze zbiorami przechowywanych i przetwarzanych danych osobowych oraz ze wskazaniem programów zastosowanych do ich przetwarzania znajduje się w załączniku nr 2.

5. Aplikacje używane do przetwarzania danych w systemie informatycznym Związku

Do przetwarzania danych w systemie informatycznym Związku stosuje się następujące aplikacje:

a) Płatnik – firmy Asseco Poland S.A.,
b) Płace - firmy QNT Systemy Informatyczne,
c) Kadry – firmy QNT Systemy Informatyczne,
d) F-K – firmy QNT Systemy Informatyczne,
e) Microsoft Office,
f) Open Office.

6. Struktura zbiorów danych aplikacji używanych do przetwarzania danych osobowych w Związku

Administrator Systemu Informatycznego posiada wydruk struktur danych (tabel) z następujących aplikacji, w których przetwarzane są dane osobowe:

a) Płatnik – firmy Asseco Poland S.A.,
b) Płace - firmy QNT Systemy Informatyczne,
c) Kadry – firmy QNT Systemy Informatyczne,
d) F-K – firmy QNT Systemy Informatyczne.

Zatwierdzam pod względem formalno-prawnym
RADCA PRAWNY
Katarzyna Potocka

7. Środki techniczne i organizacyjne służące do zapewnienia poufności i integralności danych osobowych przetwarzanych w systemie

Ochrona fizyczna

a) Urządzenia i nośniki, na których przechowywane i przetwarzane są dane osobowe znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.

b) Dostęp do pokoi jest kontrolowany poprzez wydawanie kluczy osobom posiadającym imienne upoważnienia – załącznik nr 3 - do przetwarzania danych osobowych.

c) Dokumenty w postaci papierowej oraz nośniki danych takie jak płyty CD-R / DVD-R, pamięć typu pendriv oraz wszelkie inne nośniki danych przechowywane są w zamykanych na klucz szafach.

Środki sprzętowe

a) Stosuje się niszczarki w celu niszczenia dokumentów papierowych oraz nośników optycznych CD-R / DVD-R.

b) Sieć lokalna podłączona jest do Internetu poprzez router spełniający jednocześnie funkcję zapory sprzętowej (firewall).

Oprogramowanie

a) Na komputerach użytkowników działa program antywirusowy.

b) Na komputerach użytkowników włączona jest zapora systemowa (firewall).

c) Komputery użytkowników chronione są hasłami dostępu.

Środki organizacyjne

a) Do przetwarzania danych osobowych za pomocą systemu informatycznego dopuszczane są osoby na podstawie indywidualnego pozwolenia na dostęp do przetwarzania danych osobowych.

b) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych – załącznik nr 1.

c) Osoby pracujące przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy.

d) Osoby przetwarzające dane osobowe są wcześniej szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych.

e) Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

8. Procedura postępowania w przypadku naruszenia ochrony danych osobowych

1) Pracownik Związku, który stwierdzi fakt naruszenia bezpieczeństwa danych osobowych lub posiada informacje, które mogą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to osobie pełniącej obowiązki Administratora Bezpieczeństwa Informacji.
2) W razie braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, należy zawiadomić bezpośredniego przełożonego.
3) Do czasu przybycia na miejsce Administratora Bezpieczeństwa Informacji należy:

a) zaniechać wszelkich działań mogących w następstwie utrudnić analizę naruszenia bezpieczeństwa danych osobowych,
b) jeżeli sytuacja tego wymaga, należy rozważyć wstrzymanie bieżącej pracy w celu zabezpieczenia miejsca zdarzenia,
c) ustalić przyczynę i sprawcę naruszenia ochrony danych osobowych,
d) podjąć stosowne działania, jeśli zaistniały przypadek został przewidziany w dokumentacji systemu operacyjnego, bazy danych, czy instrukcji aplikacji użytkowej,
e) jeżeli dla danego przypadku naruszenia przewidziana została instrukcja postępowania należy ją zastosować,
f) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji.

4) Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych Administrator Bezpieczeństwa Informacji podejmuje następujące kroki:

a) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Związku,
b) może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
c) jeżeli zaszła taka potrzeba informuje Administratora Danych Osobowych,
d) jeżeli zaszła taka potrzeba nawiązuje kontakt ze specjalistami spoza Związku.

Zatwierdzam pod względem formalno-prawnym
RADCA PRAWNY
Katarzyna Potocka

5) Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego załącznik nr 4, który zawiera następujące informacje:

a) określenie czasu zawiadomienia o naruszeniu bezpieczeństwa,

b) wskazanie osoby zawiadamiającej o naruszeniu, oraz innych osób zaangażowanych w wyjaśnienie okoliczności naruszenia bezpieczeństwa,

c) wskazanie lokalizacji, w której nastąpiło naruszenie bezpieczeństwa,

d) określenie rodzaju naruszenia oraz okoliczności towarzyszących,

e) wstępną ocenę przyczyn wystąpienia naruszenia,

f) podjęte działania,

g) opis postępowania wyjaśniającego.

6) Raport z naruszenia bezpieczeństwa danych osobowych Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych Osobowych.

7) Administrator Bezpieczeństwa Informacji zasięga potrzebnych mu opinii, a następnie proponuje działania naprawcze, w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń, oraz terminu wznowienia przetwarzania danych osobowych.

8) Zaistniałe naruszenie bezpieczeństwa może stać się przedmiotem zespołowej analizy. Analiza ta powinna zawierać wszechstronną ocenę zaistniałego naruszenia bezpieczeństwa, wskazanie odpowiedzialnych, wnioski co do ewentualnych działań proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

9. Postanowienia końcowe

1) Wszyscy pracownicy oraz osoby odbywające staż / praktykę w Związku, które mają dostęp do danych osobowych zobowiązane są do:

a) zapoznania się z niniejszym dokumentem,

b) przestrzegania procedur postępowania przewidzianych w przypadku naruszenia ochrony danych osobowych.

ZAŁĄCZNIK NR 1
DO POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
W ZWIĄZKU MIAST I GMIN POJEZIERZA DRAWSKIEGO
W DRAWSKU POMORSKIM

WZÓR

Ewidencja osób upoważnionych do przetwarzania danych osobowych oraz pracy w systemie informatycznym

Lp.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Id[1]	Data odebrania uprawnień i podpis ABI

[1] Identyfikator, występuje opcjonalnie jeżeli dane są przetwarzane w systemie informatycznym

10. Wobec osób, które w przypadku naruszenia ochrony danych osobowych nie podejmą odpowiednich działań (określonych w niniejszym dokumencie) podjęte zostanie postępowanie dyscyplinarne.

11. Osobom nie przestrzegającym ustawy o ochronie danych osobowych grozi odpowiedzialność karna.

12. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zapoznały się z niniejszym dokumentem – załącznik nr 5.

Zatwierdzam pod względem formalno-prawnym
RADCA PRAWNY
Katarzyna Potocka

Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe wraz z wykazem zbiorów danych osobowych oraz ze wskazaniem programów zastosowanych do ich przetwarzania

Budynek ZWIĄZKU przy ul. Piaskowej 6 w Złocieńcu

Kondygnacja	Nr pokoju	Komórka organizacyjna	Nazwa zbioru danych osobowych	Przetwarzanie danych		Program do przetwarzania danych
				W systemie informatycznym [I]	W formie papierowej [P]	
I piętro	9	Księgowość	ZUS-owskie deklaracje.		P	
			Listy płac pracowników.	I	P	Place
			Wyciągi – (rachunki bankowe)	I	P	F-K

Spis programów:

a) Płatnik – firmy Asseco Poland S.A.,
b) Płace - firmy QNT Systemu Informatyczne,
c) Kadry – firmy QNT Systemy Informatyczne,
d) F-K – firmy QNT Systemy Informatyczne
e) MS Office - Microsoft Office w skład którego wchodzą m.in. MS Word, MS Excel.
f) Open Office

Kondygnacja	Nr pokoju	Komórka organizacyjna	Nazwa zbioru danych osobowych	Przetwarzanie danych		Program do przetwarzania danych
				W systemie informatycznym [I]	W formie papierowej [P]	
I piętro	21	Kadry i administracja	ZUS-owskie kartoteki pracowników	I	P	Płatnik
			Listy płac pracowników.	I	P	Place
			Dokumentacja pracownicza	I	P	MS Office
			Umowy z wykonawcami	I	P	MS Office
I piętro	21	Zamówienia publiczne	Umowy z wykonawcami	I	P	MS Office
			Oferty	I	P	MS Office
I piętro	20	Zamówienia publiczne	Umowy z wykonawcami oraz z osobami Indywidualnymi	I	P	MS Office

Spis programów:

a) Płatnik – firmy Asseco Poland S.A.,
b) Płace - firmy QNT Systemu Informatyczne,
c) Kadry – firmy QNT Systemy Informatyczne,
d) MS Office - Microsoft Office w skład którego wchodzą m.in. MS Word, MS Excel.
e) Open Office

ZAŁĄCZNIK NR 3
DO POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
W ZWIĄZKU MIAST I GMIN POJEZIERZA DRAWSKIEGO

WZÓR

.....
(miejscowość, data)

Upoważnienie imienne do przetwarzania danych osobowych

Nr upoważnienia.....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015r. poz. 2135 z późn. zm.) upoważniam Panią / Pana.....
(imię i nazwisko osoby upoważnionej)

upoważniam zatrudnioną (ego) na stanowisku.....
do przetwarzania danych osobowych oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w Związku Miast i Gmin Pojezierza Drawskiego w zakresie
.....
.....
.....
Okres upoważnienia: .....

.....
(podpis Administratora Danych Osobowych)

Oświadczenie osoby upoważnionej

Ja niżej podpisana(y) ..... zobowiązuję się do zachowania w tajemnicy danych osobowych uzyskanych w okresie zatrudnienia / odbywania stażu / odbywania praktyki, także po ustaniu stosunku pracy / zakończenia odbywania stażu / zakończenia odbywania praktyki.

.....
(podpis składającego oświadczenie)

.....
(podpis przyjmującego oświadczenie)

ZAŁĄCZNIK NR 4
DO POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
W ZWIĄZKU MIAST I GMIN POJEZIERZA DRAWSKIEGO

WZÓR

Raport z naruszenia bezpieczeństwa danych osobowych w Związku Miast i Gmin Pojezierza Drawskiego

1. Data:..... Godzina:.....
(dd.mm.rrrr) (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:

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

5. Przyczyny wystąpienia zdarzenia:

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

6. Podjęte działania:

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

7. Postępowanie wyjaśniające:

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

.....
data, podpis Administratora Bezpieczeństwa Informacji

ZAŁĄCZNIK NR 5
DO POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
W ZWIĄZKU MIAST I GMIN POJEZIERZA DRAWSKIEGO

WZÓR

Wykaz osób, które zapoznały się z polityką bezpieczeństwa danych osobowych w Związku Miast i Gmin Pojezierza Drawskiego

Lp.	Nazwisko i imię	Stanowisko	Data	Podpis

Załącznik nr 2
do Uchwały Nr 32/2016
Zarządu Miast i Gmin Pojezierza Drawskiego
z dnia 31 sierpnia 2016 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM ZWIĄZKU MIAST I GMIN POJEZIERZA DRAWSKIEGO

-2016-

Spis treści

Załączniki

Wstęp

Instrukcja zarządzania systemem informatycznym Związku Miast i Gmin Pojezierza Drawskiego określa procedury, metody i środki przetwarzania oraz przechowywania danych osobowych w systemie informatycznym związane z zapewnieniem ich bezpieczeństwa.

Podstawa prawna dokumentu

- ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2015r. poz. 2135 z późn. zm.).
- rozporządzenie 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).

1. Definicje

- Związek – w niniejszym dokumencie oznacza Związek Miast i Gmin Pojezierza Drawskiego
- Administrator Danych Osobowych (ADO) - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. Funkcję ADO w Związku pełni Zarząd Związku
- Administrator Bezpieczeństwa Informacji (ABI) – pracownik Związku wyznaczony przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych. Funkcję ABI w Związku pełni osoba wyznaczona przez Zarząd Związku.
- Administrator Systemu Informatycznego (ASI) - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w Związku
- Użytkownik systemu – osoba która została upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być pracownik Związku, jak również osoba odbywająca staż lub praktykę w Związku
- System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

- Dane osobowe – informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
- Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, w tym zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
- Sieć lokalna (Local Area Network) – połączenie komputerów pracujących w Związku w celu wymiany danych dla potrzeb wewnętrznych, przy wykorzystaniu urządzeń sieciowych.
- Hasło – jest to ciąg znaków znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
- Identyfikator (Id) – ciąg znaków jednoznacznie identyfikujący użytkownika. W przypadku niektórych systemów odpowiednikiem Id jest nazwa użytkownika.
- Ustawa o ochronie danych osobowych - ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 z późn. zm.)

2. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

- Administrator Danych Osobowych przyznaje uprawnienia w zakresie dostępu do przetwarzania danych osobowych oraz dostępu do systemu informatycznego wystawiając pisemne upoważnienia określającego zakres uprawnień pracownika (załącznik nr 3 do Polityki bezpieczeństwa danych osobowych Związku Miast i Gmin Pojezierza Drawskiego)
- Przyznanie uprawnień w zakresie dostępu do systemu informatycznego wiąże się z wprowadzeniem do systemu dla każdego użytkownika unikalnego identyfikatora i hasła.
- Dostęp do systemu informatycznego można uzyskać jedynie po podaniu identyfikatora użytkownika oraz właściwego hasła.
- Identyfikator użytkownika nadawany jest przez Administratora Systemu Informatycznego i nie może być zmieniany bez wyraźnej przyczyny.
- Identyfikator każdego użytkownika jest unikalny. Nie można nadać identyfikatora, który został raz przydzielony innemu użytkownikowi, również w przypadku wcześniejszego wyrejestrowania tego użytkownika.
- Administrator Systemu Informatycznego przekazuje identyfikator wraz z hasłem osobie upoważnionej. Osoba ta zobowiązana jest zmienić hasło podczas pierwszego logowania się w systemie.

- Pracownik nie ma prawa do wykonywania czynności, do których nie został upoważniony.
- Administrator Systemu Informatycznego prowadzi rejestr użytkowników i ich uprawnień w systemie (załącznik nr 1).
- Odebranie uprawnień następuje na pisemny wniosek Zarządu Związku. Wniosek powinien określać termin oraz przyczynę odebrania uprawnień.
- Zarząd Związku informuje w postaci pisemnej Administratora Bezpieczeństwa Informacji, o każdej zmianie mającej wpływ na zakres uprawnień w systemie informatycznym.
- W przypadku utraty upoważnienia pracownika do dostępu do danych osobowych Administrator Systemu Informatycznego zobowiązany jest niezwłocznie zablokować dostęp do systemu informatycznego poprzez zmianę hasła lub usunięcie konta użytkownika.

3. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

- W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe na poziomie dostępu do systemu operacyjnego oraz dostępu do aplikacji służących do przetwarzania danych osobowych (z wyjątkiem aplikacji służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie).
- Użytkownik uzyskuje dostęp do systemu informatycznego jedynie po wprowadzeniu poprawnego identyfikatora i hasła.
- Stosowane hasła powinny mieć długość co najmniej 8 znaków, składać się z kombinacji małych i wielkich liter oraz cyfr, a jeżeli system na to pozwala może zawierać znaki specjalne np.: !, @, #, $, %, ^, &, *, _, -, +, ?.
- Zakazuje się stosowania haseł będących:
  - wcześniej używanym hasłem,
  - identyfikatorem użytkownika,
  - danymi osobowymi własnymi i najbliższej rodziny, takich jak: imię, nazwisko, PESEL, data urodzenia, pseudonim,
  - ogólnie dostępnych danych dotyczących użytkownika, takich jak: numer telefonu, numer rejestracyjny samochodu itp.
- Użytkownicy zobowiązani są zmieniać hasło przynajmniej raz w miesiącu, a w przypadku sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło użytkownik zobowiązany jest do natychmiastowej zmiany hasła oraz do poinformowania o zaistniałym sytuacji Administratora Bezpieczeństwa Informacji.

- Użytkownik systemu informatycznego zobowiązany jest do ochrony posiadanego hasła i ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

- Aby uzyskać dostęp do systemu informatycznego użytkownik musi podać pobrany identyfikator i hasło.
- Przed opuszczenie stanowiska użytkownik zobowiązany jest do wylogowania się z aplikacji (jeśli był w takowej załogowany), oraz wylogowania się z systemu operacyjnego.
- Przed wyłączeniem komputera użytkownik zamyka wszystkie aplikacje.
- Zakończenie pracy z systemem odbywa się przez zamknięcie systemu operacyjnego. Jeżeli system operacyjny nie przeprowadza automatycznego procesu wylogowania użytkownika, zamknięcia systemu i wyłączenia komputera - użytkownik przeprowadza te czynności w wyżej wymienionej kolejności samodzielnie.

5. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

- Za sporządzanie kopii bezpieczeństwa odpowiedzialny jest Administrator Systemu Informatycznego.
- Kopie bezpieczeństwa wykonywane są raz w tygodniu na nośniku pamięci typu flash lub na macierzy dyskowej.
- Raz w miesiącu cotygodniowe kopie bezpieczeństwa zgrywane są na płyty CD/DVD.
- Kopie w postaci płyt CD/DVD przechowywane są przez okres jednego roku.
- Po upływie roku płyty CD/DVD zostają zniszczone w sposób uniemożliwiający odczyt danych.

6. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe

- Dane osobowe w postaci elektronicznej (z wyjątkiem kopii bezpieczeństwa) zapisane na dyskietkach, płytach CD/DVD czy dyskach twardych nie mogą opuścić obszaru przetwarzania danych osobowych.

- Obszar oraz sposób przechowywania danych osobowych określony został w Polityce bezpieczeństwa danych osobowych Związku.
- Nośniki, zawierające dane osobowe, przeznaczone do likwidacji (jeżeli pozwalają na kasowanie danych) pozbawia się wcześniej tych danych, a następnie uszkadza się w sposób mechaniczny.
- Żadne nośniki informacji zawierające dane osobowe nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do używania tych danych, a w przypadku kiedy sprzęt wymaga naprawy uniemożliwiającej bezpośredni nadzór osoby upoważnionej nośniki należy uprzednio pozbawić tych danych.

7. Sposób, miejsce i okres przechowywania kopii zapasowych

- Kopie bezpieczeństwa są przechowywane w szafie w pokoju nr 21 budynku Związku
- Dostęp do danych posiada Administrator Systemu Informatycznego oraz upoważnieni pracownicy.

8. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania

- Na każdym komputerze zainstalowane jest oprogramowanie antywirusowe.
- Na każdym komputerze włączona jest zapora systemowa.
- Program antywirusowy aktualizowany jest automatycznie.
- Przynajmniej raz na trzy miesiące przeprowadzane jest skanowanie każdego komputera w poszukiwaniu wirusów.
- Kontrola antywirusowa przeprowadzana jest również w przypadku zaistnienia podejrzenia zainfekowania komputera (np. w przypadku nie prawidłowego funkcjonowania systemu).
- Zabrania się użytkownikom systemu używania nośników oraz pobierania z Internetu plików niewiadomego pochodzenia.

9. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

Aplikacje, z wyjątkiem aplikacji służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie, muszą zapewnić odnotowanie informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały

Zatwierdzam pod względem formalno-prawnym
RADCA PRAWNY
Katarzyna Potocka

udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

10. Procedury wykonywania przeglądów i konserwacji systemów informacji służących do przetwarzania danych

- Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny odbywać się zgodnie z terminami wyznaczonymi przez producenta sprzętu.
- Konserwacja aplikacji oraz baz danych powinna być przeprowadzana zgodnie z zaleceniami twórców oprogramowania.
- Prace związane z naprawami i konserwacją systemu informatycznego muszą uwzględniać wymagany poziom bezpieczeństwa danych osobowych.
- Prace związane z przeglądami, konserwacją i naprawami prowadzone na terenie Związku wykonywane mogą być jedynie przez osoby upoważnione lub pod ich bezpośrednim nadzorem.
- W przypadku przekazania nośników danych podmiotowi nieuprawnionemu do przetwarzania danych — nośniki pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.
- W przypadku kiedy w celu przeprowadzenia naprawy nośniki danych zawierających dane osobowe muszą opuścić teren Związku i nie istnieje możliwość nadzoru nad nimi osoby upoważnionej, dane te muszą zostać trwale z nich usunięte.
- W przypadku likwidacji nośników danych pozbawia się je tych danych, a w przypadku kiedy jest to niemożliwe uszkadza w sposób uniemożliwiający ich odczytanie.

11. Postanowienia końcowe

- Wszyscy pracownicy oraz osoby odbywające staż / praktykę w Związku, które mają dostęp do danych osobowych zobowiązane są do zapoznania się z niniejszym dokumentem oraz do przestrzegania procedur w nim przewidzianych.
- Wobec osób, które nie będą przestrzegały procedur (określonych w niniejszym dokumencie) podjęte zostanie postępowanie dyscyplinarne.
- Osobom nie przestrzegającym ustawy o ochronie danych osobowych grozi odpowiedzialność karna.
- Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zapoznały się z niniejszym dokumentem – załącznik nr 3.

Załącznik nr 1
do *Instrukcji zarządzania systemem informatycznym*
Związku Miast i Gmin Pojezierza Drawskiego
w Drawsku Pomorskim

Rejestr użytkowników systemu informatycznego Związku Miast i Gmin Pojezierza Drawskiego

L.p.	Imię i nazwisko	Id użytkownika	Komputery na których użytkownik posiada konto w systemie operacyjnym	Aplikacje w których użytkownik posiada konto[1]	Data nadania uprawnień	Data odebrania/zmiany uprawnień

[1] Aplikacje służących do przetwarzania danych osobowych (z wyjątkiem aplikacji służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie), w których pracownik posiada konto użytkownika.

Załącznik nr 2
do *Instrukcji zarządzania systemem informatycznym*
Związku Miast i Gmin Pojezierza Drawskiego

Dziennik systemu informatycznego Związku Miast i Gmin Pojezierza Drawskiego

L.p.	Data i godzina	Opis zdarzenia	Podjęte działania	Podpis

Załącznik nr 3
do *Instrukcji zarządzania systemem informatycznym*
Związku Miast i Gmin Pojezierza Drawskiego

WZÓR

Wykaz osób, które zapoznały się z instrukcją zarządzania systemem informatycznym w Związku Miast i Gmin Pojezierza Drawskiego

Lp.	Nazwisko i imię	Stanowisko	Data	Podpis