

**POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W MIĘDZYKŁADOWEJ KASIE  
ZAPOMOGOWO-POŻYCZKOWEJ**

przy Urzędzie Miejskim w Lidzbarku Warmińskim

**Definicje używane w niniejszym dokumencie**

**RODO** - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE - Rozporządzenie o Ochronie Danych Osobowych (EU GDPR) z dnia 27 kwietnia 2016r.

**Ustawa** - Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

**Polityka Bezpieczeństwa** – niniejszy dokument określający ogólny zakres bezpieczeństwa danych osobowych w MKZP

**Dane osobowe** – 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 powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

**Zbiór danych osobowych** - 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 osobowych** – operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

**Administrator danych osobowych** - organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 4 ust. 7 RODO, decydujące o celach i środkach przetwarzania danych osobowych.

**Pełnomocnik ds. danych osobowych** - osoba wyznaczona przez Administratora danych osobowych do prowadzenia wszelkich spraw związanych z ochroną danych osobowych.

**Interesariusz MKZP** –osoba, która ma dostęp do przetwarzanych w MKZP danych osobowych. Każdy Interesariusz MKZP mający upoważnienie do przetwarzania danych osobowych posiada swój unikalny identyfikator oraz hasło, umożliwiające zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. Techniczne wymagania, jakie musi spełniać hasło, określone zostały w **Instrukcji Zarządzania Systemem Informatycznym**.

**Obszar przetwarzania danych** – wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar/miejsce w którym są przetwarzane dane.

**MKZP** – Międzyzakładowa Kasa Zapomogowo-Pożyczkowa określona w tytule niniejszego dokumentu.

## Źródła wymagań

Polityka Bezpieczeństwa w MKZP spełnia wymagania poniższych aktów prawnych :

1. RODO,
2. Ustawa.

### § 1

Niniejszy dokument określa zasady bezpieczeństwa przetwarzania danych osobowych jakie powinny być stosowane w MKZP przez osoby przetwarzające te dane. Stosowanie Polityki bezpieczeństwa ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez MKZP rozumianej jako ochronę danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

### § 2

Interesariusz MKZP uzyskując dostęp do danych osobowych przetwarzanych w MKZP jest zobowiązany do zapoznania się z obowiązującą Polityką Bezpieczeństwa Danych.

### § 3

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych, zgodnie z Ustawą i RODO.

### § 4

Udostępnienie danych osobowych zewnętrznemu podmiotowi może nastąpić tylko po pozytywnej weryfikacji przepisów ustawowych oraz dopuszczalności takiego udostępnienia i na pisemny wniosek podmiotu uprawnionego.

### § 5

Wszelkie dokumenty w formie papierowej zawierające dane osobowe należy przechowywać w zamkniętych szafach, znajdujących się w obszarach przetwarzania danych osobowych. Niepotrzebne wydruki lub inne dokumenty należy niszczyć w sposób uniemożliwiający odczytanie ich zawartości.

### § 6

Zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym” w MKZP.

### § 7

Nadzór nad przetwarzaniem danych osobowych w MKZP sprawuje zarząd MKZP. Organ ten **może** wyznaczyć pełnomocnika ds. danych osobowych do którego zadań będzie należało bezpośrednie nadzorowanie stanu realizacji procedur związanych z ochroną danych osobowych, a w razie potrzeby także bezpośrednia realizacja procedur w imieniu zarządu KZP. W przypadku powołania Pełnomocnika ds. danych osobowych należy do niego odnosić obowiązki przewidziane w paragrafach następujących dla osoby nadzorującej przetwarzanie danych. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych osobowych. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

### § 8

Osoba nadzorująca przetwarzanie danych (Pełnomocnik ds. danych osobowych) **prowadzi następujące wykazy:**

- a) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych
- b) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania
- c) wykaz podmiotów i osób, którym udostępniono dane
- d) wykaz podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych osobowych,

#### §9

Osoba nadzorująca przetwarzanie danych (Pełnomocnik ds. danych osobowych) w ramach przetwarzania danych ma obowiązek:

- a) przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z Ustawą i RODO
- b) nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym
- c) zabezpieczać je przed zniszczeniem.

#### § 10

W przypadku zbierania danych osobowych od osoby, której one dotyczą, **osoba nadzorująca przetwarzanie danych jest obowiązana poinformować tę osobę w przystępnej dla niej formie** (w szczególności może to być informacja ustna lub zapis w umowie) o:

- a) adresie swojej siedziby i pełnej nazwie Administratora Danych Osobowych (MKZP),
- b) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- c) prawie dostępu do treści swoich danych oraz ich poprawiania,
- d) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

#### § 11

Za nieprzestrzeganie zasad ochrony danych osobowych grozi grzywna, kara ograniczenia wolności albo pozbawienia wolności zgodnie z art.107 Ustawy oraz art. 83 RODO.

#### § 12

##### 1. Procedury postępowania z danymi osobowymi

- a) dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.
- b) dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
- c) dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

##### 2. **Upoważnienie** do przetwarzania danych osobowych

- a) do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie, art. 29 RODO,
- b) upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez osobę nadzorującą przetwarzanie danych (Pełnomocnika ds. danych osobowych),
- c) upoważnienia, o których mowa powyżej, przechowywane są w aktach osobowych pracownika i obowiązują do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych.

##### 3. **Ewidencja** osób upoważnionych

- a) ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez osobę nadzorującą przetwarzanie danych (Pełnomocnika ds. danych osobowych) i zawiera w szczególności imię, nazwisko i stanowisko osoby upoważnionej do przetwarzania danych osobowych, zakres upoważnienia, data nadania i odebrania upoważnienia oraz dla osób przetwarzających dane osobowe w systemach informatycznych identyfikator użytkownika w systemie informatycznym.
- b) zarząd MKZP odpowiada za natychmiastowe zgłoszenie do ewidencji osób, które utraciły uprawnienia dostępu do danych osobowych.

##### 4. Zachowanie danych osobowych w tajemnicy

Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie pełnienia funkcji, jak również po jego ustaniu.

#### 5. Znajomość regulacji wewnętrznych

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są zapoznać się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w MKZP, w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym odpowiednią do systemu, z którego osoba będzie korzystała.

#### 6. Zgodność

Polityka Bezpieczeństwa powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach KZP, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

### §13

Osoba nadzorująca przetwarzanie danych (Pełnomocnik ds. danych osobowych) prowadzi **wykaz zbiorów danych osobowych** przetwarzanych w MKZP. W ramach nadzoru nad przetwarzaniem danych, osoba ta sprawdza w szczególności cele, zakres przetwarzania, czas przetwarzania oraz sposoby zabezpieczenia danych osobowych. Upoważnienie do przetwarzania danych osobowych nadaje osoba nadzorująca przetwarzanie danych w MKZP lub Pełnomocnik ds. danych osobowych, gdy jest wyznaczony.

### § 14

#### **ZARZĄDZANIE INCYDENTAMI**

Osoba, która zauważyła wystąpienie incydentu lub uchybienia związanego z ochroną danych osobowych, zobowiązana jest niezwłocznie poinformować osobę nadzorującą przetwarzanie danych (Pełnomocnika ds. danych osobowych) o tym fakcie. Po tym powiadomieniu osoba nadzorująca przetwarzanie danych (Pełnomocnik ds. danych osobowych) decyduje o podjęciu odpowiednich kroków:

- związanych ze zgłoszeniem incydentu do UODO,
- zmierzających do zmniejszenia skutków naruszenia (jeśli miało miejsce),
- zmiany procedur ochrony danych w celu niedopuszczenia do powtórzenia się takiego incydentu.

### § 15

#### **PRZEGLĄDY POLITYKI BEZPIECZEŃSTWA**

Polityka Bezpieczeństwa jest poddawana przeglądowi na polecenie Administratora danych osobowych. W razie istotnych zmian dotyczących przetwarzania danych osobowych, Pełnomocnik ds. danych osobowych może zarządzić przegląd bezpieczeństwa stosownie do potrzeb. W trakcie przeglądu Pełnomocnik ds. danych osobowych analizuje, czy Polityka Bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do zmian w budowie systemu informatycznego, zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych oraz zmian w obowiązującym prawie.

### § 16

W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy Ustawy oraz RODO.

#### **Wykaz załączników:**

**Załącznik Nr 2.1** - wykaz podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych.

**Załącznik Nr 2.2** – obszar przetwarzania danych osobowych, wykaz pomieszczeń w których są przetwarzane dane osobowe.

**Załącznik Nr 2.3** - wykaz zbiorów danych osobowych z dodatkowym wskazaniem programów komputerowych w których są przetwarzane dane oraz sposób przepływu danych pomiędzy poszczególnymi systemami

**Załącznik Nr 2.4** - upoważnienie do przetwarzania danych osobowych dla osób które muszą mieć dostęp do danych które podlegają ochronie, określa zakres i czas trwania upoważnienia nadawane przez Administratora Danych Osobowych lub Pełnomocnika ds. danych osobowych.

**Załącznik Nr 2.5** - oświadczenie o zachowaniu poufności zobligowane są podpisać osoby, które przetwarzają w MKZP dane osobowe, ponadto osoby te muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych (Załącznik Nr 1.4). Oświadczenie o zachowaniu poufności muszą również podpisać osoby, które wykonują doraźne prace o charakterze np. serwisowym, chyba że czynności odbywają się pod nadzorem osoby upoważnionej do przetwarzania danych.

**Załącznik Nr 2.6** - Pełnomocnictwo w celu umocowania Pełnomocnika ds. danych osobowych ma za zadanie wyznaczyć osobę do sprawowania kontroli nad wdrożeniem i realizacją Polityki Bezpieczeństwa danych w KZP, osoba taka jest wyznaczana przez Administratora Danych Osobowych - KZP (reprezentowanego przez Zarząd KZP).

**Załącznik nr 2.7** - ewidencja osób upoważnionych do przetwarzania danych osobowych – zestawienie osób, które mają dostęp do danych polegających Polityce Bezpieczeństwa.

**Załącznik nr 2.8** - wykaz udostępnień danych osobowych innym podmiotom - zestawienie osób, które uzyskały czasowy dostęp do danych polegających Polityce Bezpieczeństwa.

**Załącznik nr 2.9** - wykaz udostępnień danych osobowych osobom, których dotyczą, każda z osób podlegająca ochronie danych ma możliwość wglądu i/lub poprawiania swoich danych osobowych.

## Załącznik nr 2.1

### WYKAZ PODMIOTÓW, Z KTÓRYMI ZAWARTO UMOWY POWIERZENIA PRZETWARZANIA DANYCH

L.p.	Nazwa podmiotu	Data powierzenia	Cel powierzenia oraz numer umowy powierzenia	Jakie dane powierzono?	Określenie zbioru
1.					
2.					
3.					
4.					
5.					
6.					
7.					

## Załącznik nr 2.2

### WYKAZ POMIESZCZEŃ, W KTÓRYCH SĄ PRZETWARZANE DANE OSOBOWE

L.p.	Adres	Określenie pomieszczenia	Osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1.				
2.				
3.				
4.				
5.				
6.				
7.				

**WYKAZ ZBIORÓW DANYCH OSOBOWYCH**

L.p.	Nazwa zbioru danych	Cel przetwarzania	Nazwa aplikacji, w której przetwarzane są dane osobowe	Opis struktury zbiorów danych	Sposób przepływu danych pomiędzy aplikacjami
1.					
2.					
3.					
4.					
5.					



## Załącznik nr 2.4

Data udzielenia upoważnienia: .....

### UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Działając na podstawie przepisu art.29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. (RODO) niniejszym upoważniam Pana / Panią ..... posiadającego / posiadającą numer PESEL: ....., pełniący/pełniąca ..... funkcję ..... w KZP działającej przy .....  
.....  
.....  
do przetwarzania następujących zbiorów danych osobowych (zgodnie z załącznikiem nr 1.3):  
- .....  
- .....  
w zakresie niezbędnym do pełnienia w/w funkcji.
2. Identyfikator do logowania (w razie przetwarzania danych osobowych w systemie informatycznym):  
.....
3. Upoważnienie obowiązuje na czas pełnienia w/w funkcji lub do odwołania.
4. Osoba upoważniona do przetwarzania danych osobowych, jest zobowiązana do zachowania ich w tajemnicy, również po okresie trwania niniejszego upoważnienia.

.....  
*Data, Podpis Pełnomocnika ds. Ochrony Danych Osobowych*

**OŚWIADCZENIE**

Oświadczam, iż zapoznałem się z regulacjami prawnymi dotyczącymi ochrony danych osobowych, w szczególności z przepisami art.29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r., oraz Ustawy z dnia 10 maja 2018 r. o Ochronie Danych Osobowych w tym z zasadami odpowiedzialności karnej.

Niniejszym zobowiązuję się, zarówno w trakcie pełnienia funkcji ..... jak i po jego ustaniu, do zachowania w tajemnicy danych osobowych, do których mam lub będę miał/miała dostęp w związku z wykonywaniem czynności na rzecz Kasy Zapomogowo-Pożyczkowej (dalej zwanej KZP) przy

.....  
Ponadto, niniejszym zobowiązuję się przestrzegać wszelkich wewnętrznych zasad, procedur i wytycznych wdrożonych w KZP, dotyczących ochrony danych osobowych, w szczególności określonych w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym.

.....  
Data, Czytelny podpis

## Załącznik nr 2.6

### POWOŁANIE PEŁNOMOCNIKA DS. DANYCH OSOBOWYCH

My ..... niżej ..... podpisani  
..... jako zarząd Międzyzakładowej Kasy Zapomogowo-  
Pożyczkowej wykonujący funkcję Administratora Danych Osobowych  
niniejszym ..... upoważniamy Pana/Panią  
..... postępującego się numerem  
PESEL: .....

do sprawowania funkcji Pełnomocnika ds. danych osobowych.

Do obowiązków Pełnomocnika ds. danych osobowych będzie należało wdrożenie i nadzór nad prawidłową realizacją Polityki Bezpieczeństwa obowiązującej w KZP, w szczególności:

1. Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
2. Zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym lub zabranieniem przez osobę nieuprawnioną,
3. Zabezpieczenie danych przed ich przetwarzaniem z naruszeniem Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. (RODO) oraz Ustawy z dnia 10 maja 2018 r. o Ochronie Danych Osobowych (Ustawa) (Dz. U. z 2018 r. poz. 1000). Prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki techniczne służące ich zabezpieczeniu,
4. Wyznaczanie Administratora Systemu Informatycznego (ASI) wg zaleceń Administratora Danych Osobowych,
5. Nadawanie upoważnienia do przetwarzania danych osobowych,

.....  
Data i podpisy wszystkich członków Zarządu PKZP  
Ja, niżej podpisany, zobowiązuję się do pełnienia obowiązków Pełnomocnika ds. danych osobowych w oparciu o przepisy wewnętrzne obowiązujące w PKZP, Ustawę i RODO.

.....  
*Data i podpisy osoby przyjmującej funkcję pełnomocnika*

**Załącznik nr 2.7****EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH**

L.p.	Imię i nazwisko	Stanowisko/dział	Zakres dostępu (zgodnie z załącznikiem numer 1.4 do Polityki Bezpieczeństwa)	Okres upoważnienia Data od	Okres upoważnienia Data do	Identyfikator w systemie informatycznym
1.						
2.						
3.						
4.						
5.						
6.						
7.						

## Załącznik nr 2.8

### WYKAZ UDOSTĘPNIENÍ DANYCH OSOBOWYCH INNYM PODMIOTOM

L.p.	Imię i Nazwisko Opis osoby, której dane zostały udostępnione	Okres udostępnienia Data od / Data do	Nazwa podmiotu, któremu udostępniono dane	Cel udostępnienia (umowa nr)	Zakres udostępnionych danych	Rodzaj zbioru i jego lokalizacja
1.						
2.						
3.						
4.						
5.						
6.						
7.						

**Załącznik nr 2.9**

**WYKAZ UDOSTĘPNIENÍ DANYCH OSOBOWYCH OSOBOM, KTÓRYCH DOTYCZA**

L.p.	Imię i nazwisko	Data udostępnienia	Rodzaj zbioru i jego lokalizacja
1.			
2.			
3.			
4.			
5.			
6.			

Notatki: