# POLITYKA BEZPIECZEŃSTWA

**Lokatorsko Własnościowej**

**Spółdzielni Mieszkaniowej „Zaspa”**

**Lipiec 2018**

# SPIS TREŚCI

# ROZDZIAŁ I

# POSTANOWIENIA OGÓLNE

## § 1

### Podstawy prawne

Podstawą prawną powstania niniejszej Polityki Bezpieczeństwa jest:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 z późn. zm.), zwane w dalszej części Polityki Bezpieczeństwa „RODO".
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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), zwane w dalszej części Polityki Bezpieczeństwa „rozporządzenie Ministra MSWiA".
3. Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. 2018 r., poz. 1000).

## § 2

### Cel i zakres Polityki Bezpieczeństwa

1. **Celem Polityki Bezpieczeństwa** przetwarzania danych osobowych w **Lokatorsko Własnościowej Spółdzielni Mieszkaniowej „Zaspa"** dalej nazywaną *Polityką Bezpieczeństwa* lub *PB,* jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony przetwarzanych danych osobowych przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznym.
2. Polityka Bezpieczeństwa określa:
   a) granice dopuszczalnego zachowania podmiotów upoważnionych, w tym Użytkowników Systemu stosowanego w Lokatorsko Własnościowej Spółdzielni Mieszkaniowej „Zaspa" oraz wskazuje konsekwencje w stosunku do osób naruszających przepisy dotyczące ochrony danych osobowych,
   b) prawa i obowiązki podmiotów upoważnionych, w tym Użytkowników Systemu, w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych w nim przetwarzanych,
   c) sposób przetwarzania danych osobowych oraz środki organizacyjne i techniczne zapewniające ochronę tych danych,

d) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
e) wymagania w zakresie odnotowywania udostępniania i bezpieczeństwa przetwarzania danych osobowych,
f) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych,
g) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe (załącznik nr 1 do PB),
h) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (załącznik nr 2 do PB),
i) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (załącznik nr 2a do PB),
j) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych.

3. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   a) **poufność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom,
   b) **integralność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   c) **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   d) **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej,
   e) **dostępność informacji** - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   f) **zarządzanie ryzykiem** - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.
4. Polityka Bezpieczeństwa została wprowadzona Uchwałą Zarządu nr 3/2018 z dnia 16.07.2018r. Lokatorsko Własnościowej Spółdzielni Mieszkaniowej „Zaspa” oraz udostępniona wszystkim pracownikom.
5. Polityka Bezpieczeństwa obowiązuje wszystkie osoby upoważnione do przetwarzania danych osobowych w Lokatorsko Własnościowej Spółdzielni Mieszkaniowej „Zaspa”, bez względu na zakres udzielonego upoważnienia.

## § 3

### Definicje terminów wskazanych w Polityce Bezpieczeństwa

Definicje terminów stosowanych w niniejszej Polityce Bezpieczeństwa zgodne są definicjami wskazanymi w RODO, jak również rozporządzeniu Ministra MSWiA.
Katalog definicji:

1. **Administrator Danych Osobowych (ADO**) - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania
2. **Anonimizacja** – trwałe i nieodwracalne przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie.
3. **Dane biometryczne** - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.
4. **Dane dotyczące zdrowia** - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia.
5. **Dane genetyczne** - dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.
6. **Dane osobowe** - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
7. **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
8. **Identyfikator użytkownika** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
9. **Naruszenie ochrony danych osobowych** - 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.

10. **Osoba upoważniona do przetwarzania danych osobowych** – osoba, która została pisemnie upoważniona przez ADO do przetwarzania danych osobowych w związku z wykonywanymi przez siebie czynnościami.
11. **Podmiot przetwarzający** - osoba fizyczną lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora, na mocy umowy powierzenia przetwarzania danych osobowych.
12. **Poufności danych** - właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
13. **Profilowanie** - dowolna forma 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.
14. **Przetwarzanie** - operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.
15. **Pseudonimizacja** - 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.
16. **System informatyczny** – zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej.
17. **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
18. **Użytkownik Systemu** - podmiot posiadający indywidualną nazwę służącą do jego identyfikacji w celu umożliwienia dostępu do systemu informatycznego oraz korzystania z jego zasobów.
19. **Zbiór danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
20. **Zgoda osoby, której dane dotyczą** - 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.

## § 4

## Administrator danych osobowych

1. Administratorem danych osobowych jest **Lokatorsko Własnościowa Spółdzielnia Mieszkaniowa „Zaspa”**, al. Jana Pawła II 25C, 80-462 Gdańsk, nr KRS: 0000070340, REGON: 000484305, NIP: 5840900895, zwana również w niniejszej Polityce jako *ADO*.
2. Zgodnie z przepisami prawa na ADO ciążą między innymi następujące obowiązki:
    a. obowiązek zapewnienia bezpieczeństwa danych,
    b. obowiązek wykazania zgodności przetwarzania danych zgodnie z przepisami prawa (legalność, rozliczalność),
    c. obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,
    d. obowiązek Informacyjny zgodnie z art. 13 i 14 RODO,
    e. obowiązek umożliwienia realizacji praw osób, których dane dotyczą (prawo do bycia zapomnianym, prawo sprostowania danych, prawo dostępu do danych, prawo sprzeciwu),
    f. obowiązek zgłaszania naruszeń.
3. Administrator danych osobowych ma prawo do:
    a. upoważniania pracowników do przetwarzania danych osobowych w celu realizacji umów o pracę/zlecenie,
    b. zawierania umów o przetwarzanie danych osobowych z podmiotami zewnętrznymi,
    c. kontrolowania i monitorowania przestrzegania przepisów dotyczących ochrony danych osobowych przez podmioty wskazane powyżej,
    d. wydawania poleceń i zaleceń wszystkim upoważnionym przez siebie osobom do przetwarzania danych osobowych,
    e. wyciągania konsekwencji w stosunku do osób nieprzestrzegających postanowień zawartych w przepisach prawa, jak również niniejszej Polityce Bezpieczeństwa, w tym stosowania kar porządkowych wymienionych w Kodeksie pracy.
4. Administrator danych osobowych nie powołał Inspektora Ochrony Danych osobowych z uwagi na brak wypełnienia przesłanek wskazanych w art. 37 RODO.
5. Zakres danych osobowych przetwarzanych przez osoby upoważnione, w tym Użytkowników Systemu, nie może być szerszy niż powierzony do przetwarzania przez Administratora danych osobowych na mocy pisemnego upoważnienia, o którym mowa w §8 PB.
6. Dane osobowe przetwarzane w systemie wykorzystywane są wyłącznie w celu realizacji celów i zadań Lokatorsko Własnościowej Spółdzielni Mieszkaniowej „Zaspa” określonych w przepisach prawa spółdzielczego, Statucie oraz pozostałych aktach regulujących działalność Spółdzielni.

# RODZIAŁ II

# ZASADY PRZETWARZANIA DANYCH OSOBOWYCH. ODPOWIEDZIALNOŚĆ. OBOWIĄZEK INFORMACYJNY.

## § 5

### Zakres podmiotowy Polityki Bezpieczeństwa

Do stosowania zasad określonych przez dokument Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy Administratora danych osobowych, którzy przetwarzają dane osobowe w związku z wykonywaniem swoich obowiązków służbowych. Każda osoba, mająca dostęp do danych osobowych przetwarzanych w Lokatorsko Własnościowej Spółdzielni Mieszkaniowej „Zaspa" jest zobowiązana do zapoznania się z niniejszym dokumentem, a w razie wątpliwości, co do treści zawartych w nim postanowień, zgłoszenia niezwłocznie tego faktu Administratorowi.

## § 6

### Obszar przetwarzania danych osobowych

1. Obszarem przetwarzania danych osobowych jest siedziba Administratora danych osobowych, wskazana w §4 niniejszego dokumentu.
2. Wymagany przez rozporządzenie Ministra MSWiA wykaz budynków, pomieszczeń lub części pomieszczeń tworzących **obszar przetwarzania** danych osobowych, stanowi załącznik nr 1 do PB.
3. W przypadku zmiany lub rozszerzenia obszaru przetwarzania danych osobowych fakt ten zostaje odnotowany w odpowiednim załączniku poprzez jego zmianę lub uzupełnienie.

## § 7

### Wykaz zbiorów danych osobowych

1. Wymagany przez rozporządzenie **wykaz zbiorów danych osobowych** wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (w tym wypadku jest to rejestr czynności przetwarzania, spełniający warunki wykazu zbiorów danych), stanowi załącznik nr 2 i 2a. Sposób przepływu danych pomiędzy poszczególnymi systemami nie został określony, gdyż ADO posługuje się wyłącznie jednym systemem informatycznym (Dom 5).
2. W przypadku zmiany lub rozszerzenia zbiorów danych osobowych fakt ten zostaje odnotowany w odpowiednim załączniku poprzez jego zmianę lub uzupełnienie.

## § 8

## Upoważnienie do przetwarzania danych

1. Wszystkie osoby, które przetwarzają dane osobowe w obszarze wymienionym w § 6, muszą posiadać pisemne **upoważnienie do przetwarzania danych** nadane przez ADO (upoważnienie winno być udzielone i podpisane przez osoby reprezentujące Spółdzielnię zgodnie z treścią ujawnioną w Krajowym Rejestrze Sądowym) oraz podpisać **oświadczenie o zachowaniu poufności** tych danych, które obowiązuje także po ustaniu zatrudnienia (podpis winien być czytelny oraz opatrzony datą). Wzór upoważnienia stanowi załącznik nr 3 do PB. Wzór oświadczenia o zachowaniu poufności stanowi załącznik nr 4 do PB.
2. O udzieleniu upoważnienia decyduje wyłącznie ADO.
3. Udzielenie upoważnienia odbywa się przed dopuszczeniem pracownika do przetwarzania danych osobowych.
4. Upoważnienia do przetwarzania danych osobowych ważne są do momentu ich odwołania, do momentu upłynięcia terminu w nich wskazanych lub do chwili ustania zatrudnienia.
5. Do przetwarzania danych osobowych mogą być dopuszczeni jedynie **pracownicy** Lokatorsko Własnościowej Spółdzielni Mieszkaniowej „Zaspa" oraz pracownicy **podmiotów świadczących usługi** na jej rzecz w związku z realizacją celów i zadań Administratora, po uprzednim zawarciu z ADO umowy, o której mowa w §8.2 PB.

## § 8. 1.

## Upoważnienia do przetwarzania danych osobowych w systemie informatycznym

Upoważnieni do przetwarzania danych osobowych w systemie informatycznym są pracownicy, którzy otrzymali upoważnienia do przetwarzania danych osobowych oraz są Użytkownikami Systemu, zgodnie z definicją wskazaną w §3 ust. 16 PB.

## § 8. 2.

## Umowy powierzenia przetwarzania danych osobowych

1. Każdy podmiot wymieniony w §8 ust. 5 zobowiązany jest do podpisania z ADO umowy powierzenia przetwarzania danych osobowych, zgodnej z wymogami wskazanymi w art. 28 RODO.
2. Zakres danych osobowych powierzanych przez ADO powinien być **adekwatny do celu powierzenia** oraz **udokumentowany** w postaci wykazu podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi (załącznik nr 6 do PB).

3. Umowa z podmiotem, o którym mowa powyżej, może zostać zawarta wyłącznie w uzasadnionych potrzebami ADO przypadkach i wyłącznie po otrzymaniu od niego zapewnienia o stosowaniu odpowiednich zabezpieczeń technicznych i organizacyjnych, które gwarantują bezpieczeństwo danych.
4. Zawarcie umowy może być zainicjowane zarówno przez ADO jak i podmiot przetwarzający.

## § 9

## Zbiory danych i ogólne zasady bezpieczeństwa danych osobowych

1. W zbiorach danych przetwarzanych przez ADO (w systemie tradycyjnym oraz w systemie informatycznym) **zabrania się przetwarzania danych ujawniających**:
    a) stan zdrowia,
    b) pochodzenie rasowe lub etniczne,
    c) poglądy polityczne,
    d) przekonania religijne lub filozoficzne,
    e) przynależność wyznaniową,
    f) przynależność partyjną lub związkową,
    g) dane genetyczne,
    h) dane biometryczne,
    i) nałogi,
    j) preferencje seksualne.
2. Przetwarzanie danych, wskazanych powyżej, jest możliwe wyłącznie w przypadku wyrażenia pisemnej zgody przez osobę, której dane dotyczą lub gdy jest to niezbędne do wypełnienia obowiązków nałożonych na ADO przez przepisy prawa (prawo pracy, prawo ubezpieczeń społecznych).
3. ADO nie stosuje w prowadzonej przez siebie działalności profilowania.

## § 10

## Postępowanie z danymi. Anonimizacja i pseudonimizacja

1. Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych lub pseudonimizacji, w zależności od celu udostępniania i okresu na jaki zostały udostępnione.
3. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem przepisów (nie istnieje żadna przesłanka legalności przetwarzania danych wskazana w art. 6 RODO) lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego

upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

## § 11

## Zastosowane zabezpieczenia

1. Przed rozpoczęciem przetwarzania danych osobowych, w Lokatorsko Własnościowej Spółdzielni Mieszkaniowej „Zaspa" zastosowano środki zabezpieczające zbiory danych w postaci **zabezpieczeń technicznych i organizacyjnych** wymienionych poniżej:

a. Zabezpieczenia techniczne:
   - zbiory danych osobowych przechowywany są w pomieszczeniach zabezpieczonych drzwiami zamykanymi na klucz, do których dostęp mają tylko osoby upoważnione,
   - dane są przechowywane w pomieszczeniu, w którym okna zabezpieczone są za pomocą rolet,
   - pomieszczenia, w których przetwarzane są dane wyposażone są w system alarmowy przeciwwłamaniowy,
   - dostęp do budynku, w którym przetwarzane są dane osobowe, kontrolowany jest przez system monitoringu,
   - dane w formie papierowej przechowywane są w zamkniętej szafie, do której dostęp mają wyłącznie osoby upoważnione.
   - pomieszczenia, w których przetwarzane są dane są zabezpieczone przed skutkami pożaru za pomocą wolnostojącej gaśnicy,
   - dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.
   - dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
   - zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,
   - wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych w systemie informatycznym,
   - dostęp do danych osobowych w systemie informatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
   - zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

b. Zabezpieczenia organizacyjne:
   - do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie,

- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
- opracowano i wdrożona Politykę Bezpieczeństwa, z którą muszą zapoznać się wszystkie upoważnione osoby,
- osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
- kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,
- wprowadzono: politykę czystego biurka, politykę czystego ekranu, polityka kluczy.

## § 12

## Odpowiedzialność za naruszenia

1. Za nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialność:
   a) administracyjna (kary pieniężne nakładane na ADO),
   b) cywilna (odszkodowania z tytułu naruszenia dóbr osobistych, możliwy regres w stosunku do pracownika),
   c) karną (Zgodnie z art. 107 ustawy o ochronie danych osobowych: „*1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony ,podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.*”.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która po stwierdzeniu naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie ADO w terminie 24 godzin od momentu stwierdzenia naruszenia.

## § 13

## Obowiązek informacyjny

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, ADO jest obowiązany poinformować tą osobę o:
    a. swojej tożsamość i danych kontaktowych,
    b. celu przetwarzania danych osobowych, oraz podstawę prawną przetwarzania,
    c. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO - prawnie uzasadnione interesy realizowane przez ADO lub przez stronę trzecią,
    d. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
    e. informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
    f. 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,
    g. informacje o prawie wniesienia skargi do organu nadzorczego,
    h. informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.
2. W przypadku pozyskania danych osobowych z innego źródła, niż osoba, której dane dotyczą, ADO jest zobowiązany poinformować tę osobę o:
    a. swojej tożsamość i danych kontaktowych,
    b. celach przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania,
    c. kategoriach odnośnych danych osobowych;
    d. informacjach o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
    e. okresach, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
    f. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią,
    g. informacjach o prawie do żądania od administratora 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,
    h. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO - informacjach o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
    i. informacjach o prawie wniesienia skargi do organu nadzorczego,

j. źródłach pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych,

3. Informacje, o których mowa powyżej 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,
   c. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.

4. Obowiązek Informacyjny nie musi zostać spełniony, gdy:
   a. osoba, której dane dotyczą, dysponuje już tymi informacjami,
   b. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. 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 prawem Unii lub prawem państwa członkowskiego, któremu podlega ADO przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą,
   d. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

# ROZDZIAŁ III

# WARUNKI KORZYSTANIA Z SYSTEMU INFORMATYCZNEGO

## § 14

### Postanowienia ogólne

1. Zgodnie z postanowieniami niniejszej Polityki Bezpieczeństwa, zabrania się pracownikom ADO podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń systemu, do których nie mają dostępu.
2. Każdy Użytkownik jest zobowiązany do zapoznania się i zaakceptowania zasad korzystania z systemu informatycznego, co potwierdza własnoręczny podpis pracownika pod oświadczeniem o zapoznaniu się z PB.
3. W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego Użytkownik nie może logować się do systemu w taki sposób, aby osoba

nieupoważniona mogła poznać hasło dostępu, czy pozostawiać uruchomiony system bez zabezpieczeń.

4. Zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika.
5. Czas trwania nieaktywnej sesji (czas bezczynności) po jakim następuje automatyczne wylogowanie Użytkownika wynosi od 2 do 30 minut (czas nieaktywnej sesji uzależniony jest od charakteru wykonywanych prac przez pracowników).
6. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie dokonać zmiany hasła na nowe i poinformować o tym fakcie ADO.
7. W przypadku braku możliwości samodzielnego dokonania przez Użytkownika zmiany hasła, należy powiadomić ADO.

## ROZDZIAŁ IV
## ROZPOCZYNANIE, ZAWIESZANIE I KOŃCZENIE PRACY

### § 15

Stosuje się następujące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla Użytkowników systemu informatycznego**:**

1. Przed rozpoczęciem pracy w systemie informatycznym, należy upewnić się, że monitor jest ustawiony w sposób uniemożliwiający ujawnienia wyświetlanych danych osobom nieupoważnionym.
2. Należy upewnić się, że żadna z osób nieuprawnionych nie będzie miała możliwości zapoznania się z hasłem dostępu.
3. W przypadku zawieszenia pracy należy wylogować się z systemu i zablokować dostęp osób nieupoważnionych (tryb czuwania monitora zabezpieczony hasłem).
4. Po zakończeniu pracy należy wylogować się z systemu, a następnie wyłączyć komputer oraz monitor. Pozostawić miejsce pracy w takim stanie, aby żadna z osób nieuprawnionych nie mogła skorzystać ze sprzętu z dostępem do systemu.

## ROZDZIAŁ V

## POCZTA ELEKTRONICZNA, INTERNET W SYSTEMIE

### § 16

1. W systemie informatycznym wykorzystano funkcjonalność wysyłania powiadomień na adres e-mail podany w systemie.
2. Użytkownik zobowiązany jest do dbania o bezpieczeństwo konta mailowego, o którym mowa powyżej, w szczególności do:
   a) używania silnego hasła dostępu,
   b) nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł,
   c) zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.
3. Użytkownik zobowiązany jest do korzystania z sieci Internet w sposób, który nie zagraża bezpieczeństwu danych gromadzonych i przetwarzanych w systemie, w tym do niekorzystania z internetu w celach prywatnych (portale społecznościowe, prywatne poczty, etc.).

# ROZDZIAŁ VI

# POSTĘPOWANIE NA WYPADEK ZAGROŻENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

## § 17

### Identyfikacja zagrożeń

1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) próby naruszenia ochrony danych:
      - z zewnątrz - włamania do systemu, podsłuch, kradzież danych,
      - z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych,
   b) programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne,
   c) awarie sprzętu lub uszkodzenie oprogramowania,
   d) zabór sprzętu lub nośników z ważnymi danymi,
   e) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,
   f) usiłowanie zakłócenia działania systemu informatycznego.
2. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
   d) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

e) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
f) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

3. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach systemu zalicza się:
   a) zgłoszenia od Użytkowników,
   b) alarmy z systemów informatycznych,
   c) analizy incydentów,
   d) wyniki audytów / kontroli.

**§ 18**

**Procedura zgłaszania incydentów przez pracowników**

1. Każdy pracownik Lokatorsko Własnościowej Spółdzielni Mieszkaniowej „Zaspa", w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest niezwłocznie poinformować o tym fakcie ADO, najpóźniej w ciągu 24 godzin od wykrycia zagrożenia lub naruszenia.
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ADO lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:
   a. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
   b. zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   c. udokumentować wstępnie zaistniałe naruszenie,
   d. nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.

**§ 19**

**Procedura zgłaszania incydentów organowi nadzorczemu przez ADO**

1. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO (Prezes Urzędu Ochrony Danych Osobowych), chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Zgłoszenie, o którym mowa 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 danych osobowych, których dotyczy naruszenie,
   b. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych 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 administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

## § 20

## Postępowanie wewnętrzne

1. W przypadku stwierdzenia **wystąpienia zagrożenia**, ADO prowadzi postępowanie wyjaśniające, w toku którego:
   a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   b. inicjuje ewentualne działania dyscyplinarne,
   c. wprowadza działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
   d. dokumentuje prowadzone postępowania.

## § 21

## Podstawowe zasady bezpieczeństwa

1. Użytkownicy są zobowiązani do zachowania zasady **bezpiecznego ustawienia monitora**, czyli ustawienia go w taki sposób, aby osoby nieupoważnione nie były w stanie dostrzec informacji wyświetlających się na monitorze. Monitor powinien zostać ustawiony tyłem do drzwi oraz okna.
2. Użytkownik zobowiązany jest do przestrzegania **zasady czystego biurka**, która oznacza, że po zakończeniu pracy wszelkie dokumenty zawierające dane osobowe zostają z niego usunięte i odłożone na miejsce, w którym są przechowywane.

Zasada czystego biurka obowiązuje również w przypadku, gdy w pomieszczeniu znajdują się osoby nieuprawnione oraz, gdy nie są zastosowane żadne inne zabezpieczenia (brak pracownika przy biurku).

3. Użytkownik jest zobowiązany do przestrzegania **zasady czystej drukarki/kopiarki**, co oznacza, że po skończonej pracy polegającej na kopiowaniu dokumentów zawierających dane osobowe.

# ROZDZIAŁ VII

# MONITORING

## § 22

1. ADO, w celach zapewnienia bezpieczeństwa prowadzi w obrębie Spółdzielni Monitoring.
2. Zabronione jest monitorowanie obszarów objętych szczególną ochroną prywatności (np. toalety).
3. Zapis z monitoringu może zostać udostępniony wyłącznie na wniosek: sądu, prokuratury, organów publicznych prowadzących postępowania.
4. Zapisy z monitoringu przetwarzane są przez okres 2 tygodni, a następnie dane zostają trwale usuwane poprzez ich nadpisanie. Dopuszcza się jednak możliwość dłuższego przetwarzania danych z monitoringu, gdy dane z kamer zostały zabezpieczone na wniosek odpowiednich organów.
5. Zabronione jest odtwarzanie nagrań w obecności osób, które nie zostały upoważnione i nie złożyły oświadczenia o zachowaniu poufności.
6. W szczególnych sytuacjach dopuszcza się możliwość odtwarzania nagrań w obecności osób trzecich, ale tylko i wyłącznie w przypadku otrzymania wcześniejszego wezwania organów do zabezpieczenia nagrania. Osoba, w obecności której dokonuje się odtwarzania nagrania z monitoringu, zobowiązana jest do złożenia pisemnego oświadczenia, o którym mowa powyżej.

## § 23

## Załączniki

Integralną częścią *Polityki bezpieczeństwa są jej załączniki tj.*

- *Nr 1 Wykaz pomieszczeń, w których przetwarzane są dane osobowe (obszar),*
- *Nr 2 Rejestr czynności przetwarzania,*
- *Nr 2a Wykaz, programy oraz struktura zbiorów danych osobowych,*
- *Nr 3 Upoważnienie do przetwarzania danych osobowych,*
- *Nr 4 Oświadczenie o zachowaniu poufności,*

- *Nr 5 Wykaz osób upoważnionych do przetwarzania danych osobowych,*
- *Nr 6 Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych,*
- *Nr 7 Dziennik uchybień,*
- *Nr 8 Protokół uchybienia,*
- *Nr 9 Protokół zagrożenia,*
- *Nr 10 Oświadczenie pracownika o zapoznaniu się z zasadami ochrony danych osobowych,*
- *Nr 11 Wykaz żądań i spełnienia obowiązków ciążących na ADO.*

## ROZDZIAŁ VIII

## POSTANOWIENIA KOŃCOWE

### § 24

W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie wszelkie przepisy dotyczące ochrony danych osobowy.

### § 25

Niniejszy dokument wchodzi w życie z dniem 16.07.2018r.

……..……

podpis Administratora Danych Osobowych