**Załącznik nr 1** do Uchwały 94/2013 RADY NADZORCZEJ
SML-W z dnia **27.11.2013 roku**

# REGULAMIN

**OCHRONY DANYCH OSOBOWYCH W ZASOBACH SPÓŁDZIELNI MIESZKANIOWEJ LOKATORSKO-WŁASNOŚCIOWEJ w Konstancinie-Jeziornie.**

## I Podstawa prawna:

1. Ustawa z dnia 29.08.1997 roku o ochronie danych osobowych (Dz.U. z 2002 roku nr 101 poz. 926 tj.jedn. z późn.zm.)
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. z 2004 roku nr 100 poz. 1024).

## II Postanowienia ogólne:

**§ 1**

1. Ochrona danych osobowych w Spółdzielni Mieszkaniowej ma na celu zapewnienie każdemu członkowi Spółdzielni, osobom którym przysługują prawa do lokali w zasobach Spółdzielni i jej pracownikowi ochrony jego prywatności.
2. Regulamin niniejszy określa zasady i tryb przetwarzania danych osobowych i sposoby zabezpieczenia zbiorów danych osobowych będących w posiadaniu Spółdzielni, a także określa obowiązki administratora danych osobowych oraz prawa osób, których dane Spółdzielnia przetwarza.

**§ 2**

Użyte w niniejszym Regulaminie pojęcia oznaczają :

1. dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
2. 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 ,
3. przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie , utrwalanie , przechowywanie , opracowywanie , zmienianie , udostępnianie i usuwanie , a zwłaszcza te , które wykonuje się w systemach informatycznych,
4. system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych ,
5. zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem ,
6. usuwanie danych - zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
7. administrator danych – Zarząd Spółdzielni ,
8. zgoda osoby, której dane dotyczą - oświadczenie woli , którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie , przy czym nie może być ona domniemana lub dorozumiana z oświadczenia woli o innej treści.

**§ 3**

Celem zabezpieczenia zbiorów danych osobowych członków Spółdzielni, osób którym przysługują prawa do lokali w zasobach Spółdzielni i jej pracowników oraz ich przetwarzania jest uniemożliwienie dostępu do zbioru danych osobom nieuprawnionym bądź zbierania ich przez osobę nieuprawnioną oraz zabezpieczenie danych przed ich uszkodzeniem lub zniszczeniem.

**§ 4**

1. Spółdzielnia Mieszkaniowa jako administrator danych osobowych przetwarza dane osobowe swoich członków dla realizacji celów statutowych w zakresie:
   1/ prowadzenia rejestru członków,
   2/ prowadzenia rejestru lokali, dla których zostały założone księgi wieczyste z adnotacją o ustanowionych hipotekach oraz dokumentacji płacowej,
   3/ sporządzania list niezbędnych dla obliczenia opłat za użytkowanie lokali,
   4/ gromadzenia i przetwarzania danych osobowych zawartych w indywidualnych aktach członków Spółdzielni.
2. Spółdzielnia Mieszkaniowa jako administrator danych osobowych przetwarza dane osobowe swoich pracowników w zakresie określonym przepisami Kodeksu pracy, poprzez gromadzenie i przetwarzanie akt osobowych pracowników Spółdzielni oraz dokumentacji płacowej .

**§ 5**

1. Dostęp do zbioru danych osobowych oraz do ich przestrzegania mogą mieć wyłącznie osoby, które uzyskały pisemne upoważnienie wydane przez Zarząd Spółdzielni.

2. Zarząd Spółdzielni prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych.
3. Ewidencja, o której mowa w ust. 2 powinna zawierać:
   - imię i nazwisko pracownika,
   - stanowisko,
   - zakres w jakim stopniu został dopuszczony do przetwarzania danych osobowych,
   - datę nadania i ustania wydania upoważnienia,
   - identyfikator, w przypadku przetwarzania danych osobowych w systemie informatycznym.

   Pracownik, który uzyskał upoważnienie do dostępu danych osobowych i ich przetwarzania , powinien być zapoznany z przepisami dotyczącymi ochrony danych osobowych.
4. Pracownik Spółdzielni, który uzyskał dostęp do zbioru danych osobowych i ich przetwarzania, zobowiązany jest do złożenia oświadczenia o zachowaniu tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia przy przestrzeganiu danych osobowych.
5. Upoważnienie, o którym mowa w ust. 2 oraz oświadczenia, o których mowa w ust. 4 dołączone są do akt osobowych pracownika.
6. Indywidualny zakres czynności pracownika dopuszczanego do przetwarzania danych osobowych powinien określać jego obowiązki wynikające z czynności związanych z przetwarzaniem danych osobowych oraz zakres, w jakim pracownik został upoważniony do przetwarzania tych danych.

**§ 6**

1. Dane osobowe członków Spółdzielni, osób którym przysługują prawa do lokali w zasobach Spółdzielni i jej pracowników są przechowywane i przetwarzane w wydzielonych pomieszczeniach, określonych zarządzeniem Zarządu Spółdzielni.
2. Do pomieszczeń, o których mowa w ust. 1 mogą mieć dostęp jedynie pracownicy Spółdzielni posiadający upoważnienie Zarządu Spółdzielni.

3. Pomieszczenia, w których przechowywane i przetwarzane są dane osobowe, są zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych osobowych.

**III Ochrona danych osobowych przetwarzanych w systemach informatycznych:**

**§ 7**

1. Przy obsłudze systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być zatrudnieni wyłącznie pracownicy posiadający upoważnienie wydane przez Zarząd Spółdzielni.
2. Zarząd Spółdzielni wyznacza „administratora bezpieczeństwa informacji" odpowiedzialnego za bezpieczeństwo danych osobowych gromadzonych i przetwarzanych w systemie informatycznym.
3. Administrator bezpieczeństwa informacji odpowiedzialny jest za przeciwdziałaniu dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadkach wykrycia naruszeń w systemie zabezpieczeń.

**§ 8**

1. Pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym administratora bezpieczeństwa informacji przydziela odrębny identyfikator i hasło.
2. Identyfikator powinien być wpisany do ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych.
3. Ustalony identyfikator pracownika nie podlega zmianie w okresie jego zatrudnienia, a po wykreśleniu użytkownika z systemu informatycznego nie może być przydzielony innemu pracownikowi.
4. Hasło przydzielone pracownikowi podlega zmianie raz na miesiąc.
5. hasło powinno zawierać minimum 10 znaków, w tym litery duże i małe oraz znaki specjalne.
6. Hasło przydzielone pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych pracownik winien utrzymać w tajemnicy, także po upływie jego ważności.
7. Bezpośrednio dostęp do systemu informatycznego zawierającego dane osobowe może nastąpić wyłącznie po podaniu identyfikatora i hasła.
   Dostęp do zasobów serwera zabezpieczony jest identyfikatorem i hasłem , natomiast dostęp do systemów z danymi osobowymi posiada dodatkowe zabezpieczenie z ID i hasłem .
   Dostęp z zewnątrz jest ograniczony routerem z adresami statycznymi przypisanymi do jednostek roboczych oraz systemem Eset

8. Identyfikator osoby, która utraciła uprawnienia dostępu do systemu informatycznego zawierające dane osobowe, należy natychmiast wyrejestrować z systemu i unieważnić jej hasło.

**§ 9**

1. Pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie informatycznym obowiązany jest niezwłocznie powiadomić administratora bezpieczeństwa informacji; gdy:
   1/ stwierdzi naruszenie zabezpieczenia systemu informatycznego,
   2/ stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakości komunikacji w sieci telekomunikacyjnej mogą wskazać na naruszenie zabezpieczeń tych danych.
2. Administrator bezpieczeństwa informacji po stwierdzeniu naruszenia systemu informatycznego ma obowiązek:
   1/ zabezpieczyć ślady pozwalające na określenie przyczyn naruszenia systemu informatycznego,
   2/ przeanalizować i określić skutki naruszenia systemu informatycznego,
   3/ określić czynniki, które spowodowały naruszenie systemu informatycznego,
   4/ dokonać niezbędnych korekt w systemie informatycznym polegających na zabezpieczeniu systemu przed ponownym jego naruszeniem,
   5/ powiadomić Zarząd Spółdzielni o naruszeniu systemu informatycznego, jego przyczynach i skutkach oraz podjętych działaniach korygujących system.

**§ 10**

Administrator bezpieczeństwa informacji prowadzi rejestr pracowników- użytkowników systemu informatycznego, zawierający:
- imię i nazwisko pracownika,
- stanowisko
- zakres w jakim pracownik został dopuszczony do przetwarzania danych osobowych w systemie informatycznym,
- datę wydania upoważnienia oraz datę utraty upoważnienia,
- indywidualny identyfikator pracownika.

**§ 11**

1. System informatyczny zapewnia odnotowania
   1/ daty pierwszego wprowadzenia danych do systemu;
   2/ identyfikatora użytkownika wprowadzającego dane osobowe do systemu , chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   3/ źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   4/ informacji o osobach którym dane osobowe zostały udostępnione , dacie i zakresie tego udostępnienia,
3. Odnotowanie informacji , o których mowa w ust. 1 pkt 1) i 2 ) następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

**§ 12**

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym , system powinien zapewniać sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w paragrafie poprzedzającym .

**§ 13**

1. Zarząd Spółdzielni w drodze zarządzenia określi pomieszczenia lub ich części, tworząc obszar, w którym przetwarzane są dane osobowe w systemie informatycznym.
2. Przebywanie osób nieuprawnionych oraz dostęp do danych osobowych wewnątrz obszaru określonego w zarządzeniu Zarządu spółdzielni jest możliwe jedynie w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą Zarządu Spółdzielni.
3. Pomieszczenia, w których są przetwarzane dane osobowe, musza być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych osobowych w taki sposób, aby uniemożliwić dostęp do nich osób nieuprawnionych.
4. W pomieszczeniach, w których przebywają osoby postronne, monitory komputerów powinny być ustawione w taki sposób, żeby uniemożliwić im wgląd w dane osobowe.

**§ 14**

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

**§ 15**

Administrator bezpieczeństwa informacji obowiązany jest zabezpieczyć nośnik informacji, wydruki, kopie zapasowe, tak aby uniemożliwić dostęp do nich osobom nieuprawnionym lub przed ich uszkodzeniem lub zniszczeniem, zgodnie z przepisami.

**§ 16**

Zasady zarządzania systemem informatycznym zawierającym dane osobowe określa Instrukcja zarządzania systemem informatycznym zatwierdzona przez Zarząd Spółdzielni.

**§ 17**

1. Kopie awaryjne nie powinny być przechowywane w takich samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco, z wyjątkiem kopi codziennych .

2. Kopie awaryjne miesięczne należy przechowywać w odrębnym pomieszczeniu w specjalnym sejfie

3. Kopie awaryjne należy:
   1/ okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
   2/ bezzwłocznie usuwać po ustaniu ich użyteczności.

**§ 18**

Przetwarzane przez Spółdzielnię dane osobowe członków , osób , którym przysługują prawa do lokali w zasobach Spółdzielni i jej pracowników mogą być udostępniane osobom trzecim jedynie w przypadkach przewidzianych ustawą i na warunkach w niej wskazanych .

**§ 19**

1. Osoba, której dane przetwarzane są przez Spółdzielnię, ma prawo:
   1/ do informacji o: sposobie przetwarzania danych osobowych (ręczne przetwarzanie danych, metody informatyczne, w tym sieci komputerowej), treści danych, sposobie udostępniania danych osobowych oraz odbiorcach lub kategorii odbiorców danych,
   2/ żądania uzupełnienia, uaktualnienia i sprostowania danych osobowych.
2. Informacji, o których mowa w ust. 1 Zarząd jest zobowiązany udzielić w terminie 30 dni od daty otrzymania wniosku.

3. Postępowanie w sytuacji naruszenia ochrony danych osobowych określa Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych zatwierdzona przez Zarząd Spółdzielni.

**§ 20**

1. Niniejszy Regulamin został zatwierdzony przez Radę Nadzorczą Spółdzielni w dniu 27.11.2013 roku **Uchwałą nr 94/2013** z mocą obowiązująca od dnia **27.11.2013 roku.**
2. Z dniem wejścia w życie niniejszego Regulaminu, traci moc Regulamin Ochrony danych osobowych zatwierdzony w dniu 25.10.1999 roku Uchwałą nr 27/99 Rady Nadzorczej.

…… ……

(SEKRETARZ RADY NADZORCZEJ) (PRZEWODNICZĄCY RADY NADZORCZEJ)