

# REGULAMIN OCHRONY DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ W SEJNACH

## I. PODSTAWA PRAWNA

- 1/ Konstytucja RP.
- 2/ ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 Nr 101 poz 926 z późn.zm.)
- 3/ ustawa z dnia 16 września 1982 r. Prawo spółdzielcze (Dz.U. z 2003 Nr 188 poz 1848 z późn.zm.)
- 4/ ustawa kodeks cywilny z dnia 23 kwietnia 1964r. (Dz.U. Nr 16 poz.93 ze zm.)

## II. POSTANOWIENIA OGÓLNE

### § 1

1. Ochrona danych osobowych w Spółdzielni Mieszkaniowej w Sejnach ma na celu zapewnienie każdemu członkowi, mieszkańcom, właścicielowi lokalu, najemcy, kontrahentom, osobom skierowanym na staże oraz pracownikowi Spółdzielni ochrony jego prywatności.
2. Regulamin 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.
3. Regulamin określa zakres ochrony informacji stanowiących tajemnicę służbową, w tym tajemnicę handlową Spółdzielni, do której mają dostęp pracownicy oraz członkowie organów Spółdzielni w związku z wykonywaniem czynności służbowych lub pełnioną funkcją.

### § 2

Przez użyte w treści regulaminu sformułowania należy rozumieć :

- a) **Spółdzielnia** – Spółdzielnia Mieszkaniowa w Sejnach;
- b) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio;
- c) **zbiór danych** - to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów w szczególności : w kartotekach, skorowidzach, księgach, wykazach, rejestrach, systemach informatycznych itp.;
- d) **przetwarzanie danych** - jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

- e) **usuwanie danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
- f) **administrator danych osobowych** - podmiot zajmujący się przetwarzaniem danych osobowych, administratorem danych osobowych, o których jest mowa w §1 ust.1 jest Spółdzielnia, a w jej imieniu Prezes Zarządu Spółdzielni ;
- g) **administrator bezpieczeństwa informacji** - osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, wyznaczona przez administratora danych osobowych;
- h) **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- i) **tajemnica służbowa** - informacje w zakresie inwestycji, działalności gospodarczej i innej stanowiące tajemnicę Spółdzielni oraz informacje o kontraktach, których ujawnienie mogłoby narazić na szkodę interes Spółdzielni lub prawnie ochroniony interes innych osób lub podmiotów;

### § 3

1. Celem zabezpieczenia zbiorów danych osobowych w Spółdzielni ma na celu zapewnienie każdemu członkowi, mieszkańcom, właścicielowi lokalu, najemcy, kontrahentom oraz pracownikowi Spółdzielni jest uniemożliwienie dostępu do zbioru danych osobom nieuprawnionym bądź zabierania ich przez osobę nieuprawnioną oraz zabezpieczenie danych przed ich uszkodzeniem lub zniszczeniem.

### § 4

1. Spółdzielnia mieszkaniowa jako administrator danych osobowych przetwarza dane osobowe, o których jest mowa w §1 ust.1 dla realizacji celów statutowych w zakresie :
  - a) prowadzenia rejestru członków,
  - b) prowadzenia rejestru lokali , dla których zostały założone księgi wieczyste z adnotacją o ustanowionych hipotekach,
  - c) gromadzenia danych niezbędnych dla obliczania opłat za użytkowanie lokali,
  - d) gromadzenia i przetwarzania danych osobowych zawartych w indywidualnych aktach członków spółdzielni,
  - e) wywieszania list lokatorów i umieszczania nazwisk przy instalacji domofonowej,
  - f) gromadzenia danych innych osób posiadających prawa do lokalu,
  - g) gromadzenie niezbędnych danych do rozliczania się z kontrahentami oraz innymi podmiotami z którymi Spółdzielnia zawarła umowy,
2. Spółdzielnia jako administrator danych osobowych przetwarza dane osobowe swoich pracowników w zakresie określonym przepisami Kodeksu Pracy , poprzez gromadzenie i przetwarzanie akt osobowych pracowników Spółdzielni.

### § 5

1. Dostęp do zbioru danych osobowych oraz do ich przetwarzania mogą mieć wyłącznie osoby, które uzyskały pisemne upoważnienie wydane w imieniu Zarządu Spółdzielni przez Prezesa Zarządu. Prezes Zarządu ma prawo odebrania dostępu do zbioru danych osobowych oraz ich przetwarzania /załącznik nr 1 do regulaminu/.
2. Osoba wyznaczona przez Prezesa Zarządu Spółdzielni prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. /załącznik nr 2 do regulaminu/.
3. Ewidencja, o której mowa w ust.2, zawiera :
  - imię i nazwisko,
  - stanowisko,

- zakres, w jakim pracownik został dopuszczony do przetwarzania danych osobowych,
  - datę wydania i utraty upoważnienia,
4. Osoba, która uzyskała upoważnienie do dostępu do zbioru danych osobowych i ich przetwarzania, powinna być zapoznana z przepisami dotyczącymi ochrony danych osobowych /załącznik nr 3 do regulaminu/.
  5. Osoba, która uzyskała dostęp do zbioru danych osobowych i ich przetwarzania, zobowiązana jest do złożenia oświadczenia o zachowaniu ich w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia /załącznik nr 3 do regulaminu/.
  6. Upoważnienie, o którym mowa w ust.2 oraz oświadczenie pracownika o zachowaniu w tajemnicy danych osobowych, o których jest mowa w §1 ust.1, dołączone są do akt osobowych pracownika Spółdzielni lub osoby odbywającej staż.
  7. Indywidualny zakres czynności pracownika oraz stażysty powinien określać jego obowiązki wynikające z czynności związanych z przetwarzaniem danych osobowych oraz zakres, w jakim zostali upoważnieni do przetwarzania tych danych.

## **§ 6**

1. Pomieszczenia, w których przetwarzane są dane osobowe, muszą być zamykane na czas nieobecności w nich osób zatrudnionych w taki sposób aby uniemożliwić dostęp do nich osobom nieuprawnionym.
2. W pomieszczeniach, o których jest mowa w ust.1, w których mogą przebywać osoby postronne, monitory komputerów muszą być ustawione w sposób uniemożliwiający podgląd wyświetlanych na nich informacji. W przypadku pracy na dokumentacji papierowej uniemożliwić wgląd tym osobom do tej dokumentacji.

## **III. OCHRONA DANYCH OSOBOWYCH**

### **§ 7**

1. Obsługę systemów informatycznych oraz urządzeń wchodzących w ich skład, w których przetwarzane są dane osobowe, wykonują osoby posiadające uprawnienia, o których jest mowa w § 5.
2. Prezes Zarządu wyznacza „administratora bezpieczeństwa informacji” odpowiedzialnego za bezpieczeństwo danych osobowych gromadzonych i przetwarzanych w systemach informatycznych.
3. Administrator bezpieczeństwa informacji odpowiedzialny jest za przeciwdziałanie dostępowi osób niepowołanych do systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadkach wykrycia naruszeń w systemie zabezpieczeń.

### **§ 8**

1. Osobie, która uzyskała upoważnienie do dostępu do zbioru danych osobowych i ich przetwarzania w systemach informatycznych administrator bezpieczeństwa informacji przydziela odrębny identyfikator i hasło.
2. Nadany indywidualny identyfikator nie może być przydzielony innemu pracownikowi.
3. W przypadku utraty prawa do dostępu do zbioru danych osobowych i ich przetwarzania w systemach informatycznych administrator bezpieczeństwa informacji zobowiązany jest niezwłocznie do usunięcia z systemów identyfikatora i unieważnienia hasła.
4. Hasło powinno składać się min. 6 znaków i zawierać liczby, litery duże i małe oraz znaki specjalne.

5. Przydzielone hasło pracownik nie może udostępnić innym osobom.

## **§ 9**

1. Osoba, która uzyskała upoważnienie do dostępu do zbioru danych osobowych i ich przetwarzania w systemach informatycznych obowiązana jest niezwłocznie powiadomić administratora bezpieczeństwa informacji, gdy:
  - stwierdzi naruszenie zabezpieczenia systemów informatycznych,
  - stan urządzeń, zawartość zbioru danych osobowych, sposób działania programu lub jakości komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,
2. Administrator bezpieczeństwa informacji po stwierdzeniu naruszenia systemu informatycznego ma obowiązek:
  - a) zabezpieczyć ślady pozwalające na określenie przyczyn naruszenia systemu informatycznego,
  - b) przeanalizować i określić skutki naruszenia systemu informatycznego,
  - c) określić czynniki, które spowodowały naruszenie systemu informatycznego,
  - d) dokonać niezbędnych zmian w systemie informatycznym polegających na zabezpieczeniu systemu przed ponownym jego naruszeniem,
  - e) powiadomić Prezesa Zarządu Spółdzielni o naruszeniu systemu informatycznego, jego przyczynach i skutkach oraz podjętych działaniach,

## **§ 10**

1. Administrator bezpieczeństwa informacji prowadzi rejestr osób, które uzyskały upoważnienie do dostępu do zbioru danych osobowych i ich przetwarzania w systemach informatycznych, który zawiera:
  - a) imię i nazwisko,
  - b) datę wydania upoważnienia,
  - c) datę utraty upoważnienia,
  - d) indywidualny identyfikator pracownika,
  - e) hasło,

## **§ 11**

1. 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.

## **§ 12**

1. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
3. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

4. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

### **§ 13**

1. Kopie awaryjne, sporządza administrator bezpieczeństwa informacji na przenośnych urządzeniach rejestrujących minimum 1 raz w miesiącu.
2. Kopie awaryjne nie mogą być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
3. Kopie awaryjne należy:
  - a) okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu,
  - b) bezzwłocznie usuwać po ustaniu ich użyteczności.

### **§ 14**

1. Administrator bezpieczeństwa informacji minimum raz w miesiącu dokonuje osobistego sprawdzenia systemów komputerowych pod kątem wykrycia wirusów komputerowych i innego złośliwego oprogramowania.
2. Przeglądy i konserwacja systemu i zbioru danych osobowych dokonywane są przez administrator bezpieczeństwa informacji minimum 1 raz w miesiącu.
3. Z czynności określonych w ust. 1 – 2 administrator bezpieczeństwa informacji sporządza pisemną informację i przedstawia ją do zatwierdzenia Prezesowi Zarządu.

## **IV. OCHRONA TAJEMNICY SŁUŻBOWEJ**

### **§ 15**

1. Informacje o działalności prowadzonej przez Spółdzielnię, a w szczególności dotyczące: prowadzonych inwestycji, planów inwestycyjnych, działalności gospodarczej - stanowią tajemnicę służbową.
2. Tajemnicą służbową w tym handlową w Spółdzielni objęte są również informacje będące w posiadaniu Spółdzielni i dotyczące jej kontrahentów, w szczególności: informacje o adresach prywatnych osób reprezentujących kontrahenta, stosowane przez niego technologie, jego sytuacja finansowa, osiągnięte obroty przedsiębiorstwa, informacje o ofertach i kontrahentach handlowych i inne.
3. Pracownicy i członkowie organów samorządowych Spółdzielni zobowiązani są do złożenia pisemnego oświadczenia o zachowaniu w tajemnicy danych osobowych i informacji stanowiących tajemnicę służbową w tym handlową.

## **V. UDOŚTĘPNIANIE DANYCH OSOBOWYCH I INFORMACJI STANOWIĄCYCH TAJEMNICĘ SŁUŻBOWĄ**

### **§ 16**

1. Zarząd Spółdzielni może udostępnić dane osobowe członka spółdzielni Walnemu Zgromadzeniu (Zebraniu Przedstawicieli), Radzie Nadzorczej jedynie w przypadku, gdy

w sprawie danego członka toczy się postępowanie wewnątrzspółdzielcze lub rozpatrywana jest jego sprawa w postępowaniu wewnątrzspółdzielczym, ale tylko w zakresie mogącym mieć znaczenie dla danej sprawy.

2. Zarząd Spółdzielni jest zobowiązany do poinformowania członków organów samorządowych spółdzielni rozpatrujących sprawę członka spółdzielni w postępowaniu wewnątrzspółdzielczym o przepisach dotyczących ochrony danych osobowych.
3. Zarząd Spółdzielni jest zobowiązany udostępnić Radzie Nadzorczej wszelkie sprawozdania i księgi oraz dokumenty dotyczące działalności statutowej Spółdzielni. Prawo wglądu we wszystkie dokumenty, księgi i sprawozdania przysługuje Radzie Nadzorczej jako organowi kolegialnemu.
4. Indywidualni członkowie Rady Nadzorczej mogą korzystać z tego prawa, jeżeli zostali do tego upoważnieni uchwałą organu powierzającego im przeprowadzenie badań określonej dziedziny działalności Spółdzielni, których wyniki mogą być przedstawiane do oceny organu.
5. Dokumenty udostępnione organom samorządowym nie mogą być wynoszone poza siedzibę Spółdzielni w żadnej postaci tj. oryginałów, kserokopii czy odpisów.
6. W przypadku podjęcia przez Radę Nadzorczą uchwały o zleceniu badania dokumentów, sporządzania ekspertyzy lub opinii uprawnionym specjalistom - biegłym, dokumenty wskazane przez Radę Nadzorczą przygotowuje (sporządza kopie) i parafuje upoważniony przez Zarząd pracownik Spółdzielni.
7. Zarząd Spółdzielni jest zobowiązany do poinformowania członków organów samorządowych Spółdzielni rozpatrujących sprawę członka Spółdzielni w postępowaniu wewnątrzspółdzielczym o przepisach dotyczących prawnej ochrony danych osobowych, a także informacji stanowiących tajemnicę służbową w tym handlową oraz tajemnicę przedsiębiorstwa kontrahentów Spółdzielni.

## § 17

1. Udostępnienie danych osobowych przetwarzanych przez Spółdzielnię osobom fizycznym lub instytucjom publicznym może nastąpić jedynie na piśmie umotywowany wniosek, chyba że przepis szczegółowy stanowi inaczej.
2. Wniosek, o którym mowa w ust. 1 może jedynie dotyczyć konkretnej osoby w konkretnej sytuacji i powinien być zgodny z wnioskiem opublikowanym jako załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia wniosków o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej Inspektora Biura Generalnego, Inspektora Danych Osobowych - Dz. U. Nr 80 poz. 522 ze zm.
3. Spółdzielnia może odmówić udostępnienia danych osobowych, o których jest mowa w §1 ust.1 w przypadkach określonych w Ustawie o ochronie danych osobowych - art. 34.
4. Umieszczenie nazwiska członka Spółdzielni lub osoby posiadającej tytuł prawny do lokalu w budynku wchodzącym w skład nieruchomości będącej w zarządzie Spółdzielni na liście lokatorów lub przy instalacji domofonowej jest możliwe po wyrażeniu pisemnej zgody przez członka Spółdzielni lub

osobę posiadającą tytuł prawny do lokalu w budynku wchodzącym w skład nieruchomości będącej w zarządzie Spółdzielni

### **§ 18**

1. Osoba, której dane przetwarzane są przez Spółdzielnię, ma prawo do informacji o:
  - a) sposobie przetwarzania danych osobowych (ręczne przetwarzanie danych , teleinformatyczne przetwarzanie danych, w tym w sieci komputerowej),
  - b) treści danych,
  - c) sposobie udostępniania danych osobowych oraz odbiorcach lub kategorii odbiorców danych,
2. Osoba, o której mowa w ust. 1 ma prawo żądania uzupełniania, uaktualniania i sprostowania danych osobowych.
3. Informacji, o których mowa w ust.1 Spółdzielnia , jest zobowiązana udzielić w terminie 30 dni od daty otrzymania wniosku.

## **VI. POSTANOWIENIA KOŃCOWE**

### **§ 19**

1. W sprawach nieuregulowanych Regulaminem mają zastosowanie odpowiednie przepisy Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych z późniejszymi zmianami oraz innych aktów prawnych dotyczących ochrony danych osobowych

### **§ 20**

1. Traci moc Regulamin ochrony danych osobowych w Spółdzielni Mieszkaniowej w Sejnach uchwałą Rady Nadzorczej Nr 15/99 z dnia 29 października 1999 r.

**Sekretarz Rady Nadzorczej**

**Przewodniczący Rady Nadzorczej**

.....

.....

Załącznik nr 1 do Regulaminu

.....  
/pieczętka zakładu pracy/

## UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych (Dz. U. z 1997r nr. 133, poz. 883 z późn. zm.) i na podstawie § 5 pkt. 1 Regulaminu ochrony danych osobowych Spółdzielni Mieszkaniowej w Sejnach, upoważniam Pana(ią) ..... do dostępu do zbioru danych osobowych i ich przetwarzania w celu .....

.....  
(data i podpis Prezesa Zarządu)

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych (Dz. U. z 1997r nr. 133, poz. 883) i na podstawie § 5 pkt. 1 Regulaminu ochrony danych osobowych



Spółdzielni Mieszkaniowej w Sejnach, odbieram Panu(i) .....  
dostęp do zbioru danych osobowych i ich przetwarzania.

.....  
(data i podpis Prezesa Zarządu)

Załącznik nr 2 do Regulaminu

.....  
/pieczęć zakładu pracy/

#### Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	imię i nazwisko	stanowisko	zakres przetwarzania danych osobowych	data nadania uprawnień	data utraty uprawnień

Załącznik nr 3 do Regulaminu

Ja niżej podpisany(a) oświadczam, że znana mi jest treść Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i zobowiązuję się nie ujawniać nikomu w żaden sposób i nie wykorzystywać informacji związanych z przetwarzanymi danymi osobowymi, z którymi się zapoznałem(am) w związku z wykonywaną pracą przez okres zatrudnienia, stażu lub pełnionych funkcji w statutowych organach SM, jak i po ich ustaniu.

.....