**LOKATORSKA SPÓŁDZIELNIA MIESZKANIOWA**
**W KRAKOWIE**
**30-428 KRAKÓW, UL. ZDUNÓW 18A/1**

# REGULAMIN OCHRONY DANYCH OSOBOWYCH

KRAKÓW, LUTY 2010r.

# REGULAMIN OCHRONY DANYCH OSOBOWYCH LOKATORSKIEJ SPÓŁDZIELNI MIESZKANIOWEJ W KRAKOWIE

## I. POSTANOWIENIA OGÓLNE

Niniejszy regulamin opracowany został dla Lokatorskiej Spółdzielni Mieszkaniowej w Krakowie (dalej także: „**Spółdzielnia**", „**LSM**") na podstawie Ustawy z dnia 29.08.1997r. (tekst jednolity Dz.U. z 2002r. Nr 101 poz 926 z późn. zm.) o ochronie danych osobowych oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. (Dz.U. z 2004r. Nr 100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych.

§ 1

Regulamin niniejszy określa zasady, 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

Przez użyte w treści regulaminu sformułowania należy rozumieć:

1) **dane osobowe** – każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby;
2) **zbiór danych** – każdy posiadający strukturę zestaw danych osobowych dostępny według określonych kryteriów, w których dane są przetwarzane, w szczególności: w kartotekach, skorowidzach, księgach, wykazach, rejestrach, systemach informatycznych itp.;
3) **przetwarzanie danych** – wszelkie operacje wykonywane na danych osobowych i ich zbiorach, w szczególności: zbieranie, utrwalanie, przechowywanie, opracowanie, zmienianie, udostępnianie i usuwanie danych osobowych;
4) **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby której dane dotyczą;
5) **administrator danych osobowych** – podmiot zajmujący się przetwarzaniem danych osobowych. Administratorem danych osobowych członków Spółdzielni i jej pracowników jest Spółdzielnia, a w jej imieniu Zarząd Spółdzielni;
6) **administrator bezpieczeństwa informacji** – osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, wyznaczona przez administratora danych osobowych;
7) **system informatyczny** – system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, których dostarcza i rozprowadza informacje.

§ 3

Celem zabezpieczenia zbiorów danych osobowych członków Spółdzielni i innych użytkowników lokali Spółdzielni oraz jej pracowników 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 jako administrator danych osobowych przetwarza dane osobowe swoich członków dla realizacji celów statutowych w zakresie:
   1) prowadzenia rejestru członków
   2) prowadzenia ewidencji mieszkańców budynku
   3) prowadzenia ewidencji najemców lokali mieszkalnych, użytkowych i garaży
   4) prowadzenie rejestru lokali, dla których zostały założone księgi wieczyste z adnotacją o ustanowionych hipotekach
   5) sporządzania list niezbędnych dla obliczania opłat za użytkowanie lokali
   6) sporządzanie wykazów niezbędnych do rozliczeń z członkami z tytułu wkładów budowlanych i mieszkaniowych, kredytów oraz kaucji
   7) gromadzenia i przetwarzania danych osobowych zawartych w indywidualnych aktach członków spółdzielni
   8) wywieszania list lokatorów i umieszczania nazwisk przy instalacji domofonowej
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. Do przetwarzania danych osobowych uprawnieni są:
   a) osoby, które w oparciu o umowę o pracę i zakres czynności odpowiadają za prawidłowe i zgodne z obowiązującymi przepisami wykorzystanie informacji ze zbioru danych realizujący określone zadania Spółdzielni,
   b) osoby fizyczne i prawne, które na podstawie umów cywilnoprawnych zawartych ze Spółdzielnią realizują zlecone przez Spółdzielnię zadania a dane osobowe ze zbioru danych są im niezbędne do wykonania przedmiotu umowy,
2. Do przetwarzania danych osobowych w systemie informatycznym mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez Zarząd Spółdzielni. Upoważnienie powinno zawierać zakres przetwarzania danych.
3. Pracownicy Spółdzielni oraz członkowie organów samorządowych Spółdzielni są zobowiązani do zachowania w tajemnicy uzyskanych informacji wynikających z przetwarzania danych osobowych i z dostępu do tych danych w czasie wykonywania obowiązków pracowniczych lub zadań wynikających z uprawnień statutowych członka organu samorządowego Spółdzielni.
4. 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 przy przetwarzaniu danych osobowych.

5. Indywidualny zakres czynności pracownika dopuszczonego do przetwarzania danych osobowych powinien określać jego obowiązki wynikające z czynności związanych z przetwarzaniem danych osobowych oraz ustalać zakres odpowiedzialności tej osoby za ich ochronę.
6. Upoważnienie, o którym mowa w ustępie 2, oraz oświadczenie pracownika o zachowaniu tajemnicy danych osobowych członków Spółdzielni i jej pracowników, dołącza się do akt osobowych pracownika – wzory oświadczeń w załączeniu – **Załącznik nr 1**.
7. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych.

§ 6

1. Zarząd Spółdzielni może udostępnić dane osobowe członka Spółdzielni Walnemu Zgromadzeniu i/lub Radzie Nadzorczej jedynie w przypadku, gdy w sprawie danego członka toczy się postępowanie wewnątrzspółdzielcze w trybie określonym postanowieniami statutu Spółdzielni.
2. Dane osobowe członka Spółdzielni mogą być udostępnione organom samorządowym Spółdzielni rozpatrującym jego sprawę w postępowaniu wewnątrzspółdzielczym tylko w zakresie mogącym mieć znaczenie dla danej sprawy.
3. Zarząd Spółdzielni jest zobowiązany do poinformowania członków organów samorządowych Spółdzielni rozpatrującym sprawę członka Spółdzielni w postępowaniu wewnątrzspółdzielczym o przepisach dotyczących ochrony danych osobowych.
4. Udostępnienie danych osobowych przetwarzanych przez Spółdzielnię osobom fizycznym lub instytucjom publicznym uprawnionym do ich otrzymania na mocy przepisów prawa może nastąpić jedynie na pisemnie umotywowany wniosek chyba, że przepis szczególny stanowi inaczej – wzór wniosku w załączeniu – **Załącznik nr 2**.
5. Wniosek, o którym mowa w ust. 4 powyżej, powinien zawierać informacje umożliwiające wyszukiwanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

§ 7

Administrując zbiorami danych wymienionych w § 4 Spółdzielnia jest obowiązana stosować wymienione zasady udostępniania danych określone w § 6 z uwzględnieniem dodatkowych wskazówek:

1) zgodnie z art. 30 prawa spółdzielczego każdy członek ma prawo przeglądać rejestr członków Spółdzielni
2) wywieszenie list lokatorów w klatkach schodowych lub przy domofonie wymaga zgody lokatorów na umieszczenie ich nazwisk na wskazanych listach,

3) wgląd do wszystkich danych osobowych tworzonych w Spółdzielni mogą mieć tylko osoby, których te dane dotyczą i osoby upoważnione przez Zarząd do ich gromadzenia i przetwarzania.

§ 8

1. Przekazanie danych osobowych do państwa trzeciego może nastąpić jedynie wtedy, jeżeli państwo docelowe daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jak obowiązujące na terytorium Rzeczypospolitej Polskiej.
2. Przepisu ust. 1 nie stosuje się, gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej.
3. Administrator danych może jednak przekazać dane osobowe do państwa trzeciego, jeżeli:
   1. osoba, której dane dotyczą, udzieliła na to zgody na piśmie,
   2. przekazanie jest niezbędne do wykonywania umowy pomiędzy administratorem danych a osobą, której te dane dotyczą, lub jest podejmowane na jej życzenie,
   3. przekazanie jest niezbędne do wykonywania umowy zawartej w interesie osoby, której te dane dotyczą, pomiędzy administratorem danych a innym podmiotem,
   4. przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych,
   5. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,
   6. dane są ogólnie dostępne
4. W przypadkach innych niż wymienione w § 8 ust. 2 i 3 Regulaminu przekazanie danych osobowych do państwa trzeciego, który nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może mieć miejsce po uzyskaniu zgody Generalnego Inspektora Ochrony Danych Osobowych, pod warunkiem, że administrator danych zapewni odpowiednie zabezpieczenia w zakresie prywatności oraz praw i wolności osoby, której te dane dotyczą.

§ 9

1. Dla zapewnienia prawidłowego, zgodnego z ustawą przetwarzania zbioru danych osobowych Administrator danych osobowych wyznacza osobę – zwaną dalej „Administratorem bezpieczeństwa informacji" odpowiedzialną za bezpieczeństwo danych w systemie informatycznym.
2. Administratorem bezpieczeństwa informacji może być:
   a) pracownik Spółdzielni zatrudniony na podstawie umowy o pracę
   b) podmiot, posiadający uprawnienia do świadczenia usług w zakresie wymaganym ustawą, z którym Spółdzielnia zawarła umowę cywilno-

prawną a przedmiot umowy obejmuje zakres obowiązków wynikający z ustawy o ochronie danych osobowych.

§ 10

W sytuacji stwierdzenia naruszenia zabezpieczenia danych należy zabezpieczyć pomieszczenia, szafy, dokumenty przed dostępem osób trzecich i niezwłocznie powiadomić Zarząd Spółdzielni, który według własnej oceny sytuacji podejmie stosowne działania.

## II. OCHRONA DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM

§ 11

1. Zbiór danych osobowych w systemie informatycznym to „dane informatyczne", w których źródłem są informacje zapisane na nośnikach informatycznych (dyskach, dyskietkach) wykorzystywane do prowadzenia zgodnej z obowiązującymi przepisami działalności Spółdzielni w zakresie określonym w Prawie Spółdzielczym, Kodeksie pracy i innych przepisach stanowiących podstawę prawną funkcjonowania Spółdzielni.
2. Administrator bezpieczeństwa informacji odpowiedzialny jest za przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadkach wykrycia naruszeń w systemie zabezpieczeń.

§ 12

1. Pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym Administrator bezpieczeństwa informacji przydziela odrębny identyfikator i hasło.
2. Ustalony identyfikator pracownika nie podlega zmianie w okresie jego zatrudnienia, a po wykreśleniu użytkownika z systemu informatycznego nie może być przydzielony innemu pracownikowi.
3. Hasło przydzielane pracownikowi podlega zmianie w terminie ustalonym przez Zarząd Spółdzielni.
4. Bezpośredni dostęp do systemu informatycznego zawierającego dane osobowe może nastąpić wyłącznie po podaniu identyfikatora i hasła.
5. Identyfikator osoby, która utraciła uprawnienia dostępu do systemu informatycznego zawierającego dane osobowe, należy natychmiast wyrejestrować z systemu i unieważnić jej hasło.
6. 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.

§ 13

Ewidencja przebiegu przetwarzania danych winna być prowadzona poprzez:

- Ewidencję daty i ostatniego zapisu każdego aktualizowanego zbioru
- Ewidencję daty sporządzenia ostatniego pliku zawierającego aktualną kopię wszystkich zbiorów
- Ewidencję daty ostatniej wersji programów systemu
- Tworzenie zbioru na dysku twardym, w którym odnotowuje m.in.:
  - datę uruchomienia programu
  - informację, czy przebieg przetwarzania zakończył się prawidłowo i poprawnie
  - ewentualne miejsce w programie, w którym przebieg przetwarzania został przerwany lub zakończył się niepoprawnie
  - przyczyny przerwania przebiegu przetwarzania danych
  - zakończenie przebiegu przetwarzania

§ 14

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

§ 15

1. Urządzenia, dyski i inne nośniki informatyczne zawierające dane osobowe przeznaczone do naprawy lub przekazania innemu podmiotowi pozbawia się zapisu danych.
2. Dysk i inne nośniki informatyczne zawierające dane osobowe do likwidacji pozbawia się wcześniej zapisanych danych a gdy nie jest to możliwe uszkadza się je w sposób uniemożliwiający odczyt.

§ 16

Administrator bezpieczeństwa informacji obowiązany jest zabezpieczyć nośniki informacji, wydruki, kopie zapasowe, tak aby uniemożliwić dostęp do nich osobom nieuprawnionym lub chronić je przed ich uszkodzeniem lub zniszczeniem

§ 17

1. Kopie awaryjne powinny być tworzone na bieżąco nie rzadziej niż jeden raz na dwa miesiące poprzez przegranie danych na zapasowe dyski twarde przez firmę komputerową obsługującą Spółdzielnie oraz poprzez przeniesienie danych na dyskietki/płyty CD, DVD/dyski przenośne przez pracowników obsługujących poszczególne programy komputerowe.

2. Kopie awaryjne nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
3. Kopie awaryjne należy:
   1) okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu
   2) bezzwłocznie usuwać po ustaniu ich użyteczności
4. W celu zabezpieczenia zbiorów danych przed uszkodzeniem lub zniszczeniem na skutek wprowadzenia wirusów komputerowych – Spółdzielnia powinna być zaopatrzona w programy antywirusowe.
5. Nośniki informatyczne w postaci dysków i dyskietek komputerowych oraz wydruki komputerowe winny być przechowywane przez okres wynikający z kategorii zaszeregowania do odpowiedniej grupy dokumentów z punktu widzenia przepisów o archiwach państwowych.
6. Przeglądy i konserwacje systemu informatycznego Spółdzielni prowadzone są zgodnie z zawartymi w tym zakresie umowami przez firmy komputerowe obsługujące Spółdzielnię.

§ 18

1. W Spółdzielni rozróżnia się następujące kategorie zabezpieczeń danych osobowych:
   a) Zabezpieczenia fizyczne:
      - pomieszczenia, w których przetwarzane są dane zamykane są przed i po zakończeniu godzin pracy,
      - budynek, w którym znajdują się pomieszczenia jest dodatkowo chroniony systemem alarmowym,
      - monitory są ustawione w ten sposób, by uniemożliwić wgląd do danych osobom trzecim.
   b) Zabezpieczenia przetwarzania danych w dokumentacji:
      - dokumenty i inne nośniki zawierające dane osobowe i informacje poufne są składowane w zamykanych szafach,
      - samodzielny dostęp do pomieszczeń, w których przetwarzane są dane osobowe posiadają jedynie osoby posiadające odpowiednie upoważnienie,
      - przebywanie osób nieupoważnionych w pomieszczeniach jest możliwe wyłącznie za zgodą administratora bezpieczeństwa informacji lub w towarzystwie osoby upoważnionej,
   c) Zabezpieczenia organizacyjne:
      - osobą odpowiedzialną za bezpieczeństwo danych w Spółdzielni jest Administrator Bezpieczeństwa Informacji, który opracowuje dokumentację wewnętrzną: Politykę bezpieczeństwa oraz Instrukcję zarządzania systemem informatycznym i na bieżąco kontroluje pracę systemu informatycznego oraz przestrzegania zasad ochrony informacji,
      - w przypadkach wykrycia rażących zaniedbań w tym zakresie, Administrator Bezpieczeństwa Informacji sporządza ich opis i niezwłocznie przedkłada Zarządowi Spółdzielni.

d) Zabezpieczenia dotyczące pracowników i organizacji pracy:
- pracownicy, jak i osoby mające dostęp do zbiorów winni być zaznajomieni z powszechnie obowiązującymi przepisami dotyczącymi przetwarzania danych osobowych oraz procedurami wewnętrznymi określonymi w dokumentacji przetwarzania danych osobowych,
- pracownicy, jak i osoby mające dostęp do danych osobowych, które są w dyspozycji Spółdzielni zobowiązani są do utrzymywania w tajemnicy wszystkich uzyskanych informacji w szczególności w zakresie stosowanych zabezpieczeń systemu informatycznego (zakaz ujawniania informacji dotyczy zarówno ujawniania informacji osobom trzecim, jak również wszystkim pracownikom, którzy nie posiadają upoważnienia do przetwarzania danych),
- pracownicy przetwarzający dane osobowe powinni posiadać Upoważnienie do przetwarzania danych osobowych w określonym w nim zakresie, wydane przez Zarząd Spółdzielni. Upoważnienie dołącza się do akt osobowych pracownika. Wzory Upoważnień w załączeniu – **Załącznik nr 3**. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji,
- pracownicy zatrudnieni przy przetwarzaniu danych osobowych, jak i osoby mające dostęp do danych osobowych są zobowiązani do podpisania stosownego zobowiązania do zachowania tajemnicy,
- istnieje zakaz ujawniania i udostępniania haseł osobom trzecim.

2. W ramach zabezpieczenia danych osobowych ochronie podlegają:
   1) sprzęt komputerowy – serwer i urządzenia zewnętrzne,
   2) oprogramowanie,
   3) dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie,
   4) hasła użytkowników,
   5) bazy danych i kopie zapasowe,
   6) wydruki,
   7) związana z przetwarzaniem danych dokumentacja papierowa.

§ 19

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 wskazywać 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

§ 20

Do regulaminu załącza się:
1. **Załącznik nr 1** - Wzór upoważnienia użytkownika systemu informatycznego
2. **Załącznik nr 2** - Wzór wniosku o udostępnienie danych ze zbioru danych osobowych
3. **Załącznik nr 3** - Wzór oświadczenia o zachowaniu danych osobowych w tajemnicy

§ 21

1. Niniejszy Regulamin został zatwierdzony przez Radę Nadzorczą w dniu 09.02.2010 r. Uchwałą Nr 81/III/2010.
2. Postanowienia Regulaminu wchodzą w życie z dniem podjęcia Uchwały przez Radę Nadzorczą.

**WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH**
do LOKATORSKIEJ SPÓŁDZIELNI MIESZKANIOWEJ w Krakowie

Wnioskodawca:.....

.....
( nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON )

Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych osób innych niż wymienione w art.29 ust. 1 ustawy o ochronie danych osobowych.

.....

.....

.....

Wskazanie przeznaczenia dla udostępnionych danych.....

.....

Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:.....

.....

Zakres żądanych informacji ze zbioru: .....

.....

.....

.....

Informacje umożliwiające wyszukanie w zbiorze żądanych danych: .....

.....

.....

.....

.....

.....

Kraków, dnia .....r.

.....
(podpis i ew. pieczęć wnioskodawcy)

# UPOWAŻNIENIE

Zarząd Spółdzielni Lokatorskiej Spółdzielni Mieszkaniowej w Krakowie upoważnia Pana / Panią .....

.....

do obsługi komputera i przetwarzania danych osobowych w zakresie .....

.....

.....

.....

.....

.....

Równocześnie zobowiązuje się Pana / Panią do ochrony danych osobowych uzyskanych w czasie wykonywania powyższego zakresu zadań związanych z przetwarzaniem danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją, zniszczeniem lub nielegalnym ujawnieniem i pozyskiwaniem danych.

Kraków, dnia .....r.

.....
(podpis i ew. pieczęć osoby wystawiającej upoważnienie)

# OŚWIADCZENIE

1. Świadomy / a odpowiedzialności karnej oświadczam, że uzyskane informacje wynikające z przetwarzania danych osobowych i z dostępu do tych danych w czasie wykonywanych obowiązków pracowniczych – pracy zleconej- zadań wynikających z uprawnień statutowych członka organu samorządowego * / - zachowam w tajemnicy.

2. Zobowiązuję się zachować w tajemnicy te informacje również po ustaniu zatrudnienia – -pracy w organie samorządowym Spółdzielni */.

3. Potwierdzam, że zostałem /am zapoznany / a z przepisami o ochronie danych osobowych obowiązujących w Spółdzielni.

Kraków, dnia .....r.

.....
(podpis)

*/ niepotrzebne skreślić