REGULAMIN OCHRONY DANYCH OSOBOWYCH

Spółdzielni Mieszkaniowej „CENTRUM”

§ 1

Regulamin ochrony danych osobowych - dalej zwany "Regulaminem" - opracowano w oparciu o powszechnie obowiązujące przepisy prawa, a w szczególności w oparciu o:

1.Ustawę z dnia 29.08.1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. Nr 101 poz. 926, z 2002 r. z późniejszymi zmianami),
2.Ustawę z dnia 16 września 1982 r. - Prawo spółdzielcze (tekst jednolity Dz.U. Nr 188 poz. 1848 z 2003 r. z późniejszymi zmianami),
3. Ustawę z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (tekst jednolity Dz. U. Nr 119 poz. 1116 z 2003 r. z późniejszymi zmianami),
4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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 poz. wraz z późniejszymi zmianami),
5.Ustawę z dnia 26 czerwca 1974 r. – Kodeks pracy (tekst jednolity Dz.U. Nr 21 poz. 94 z1998 r. z późniejszymi zmianami),
6. Ustawę z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tekst jednolity Dz.U. Nr poz. z r. z późniejszymi zmianami),
7.Statut Spółdzielni Mieszkaniowej „CENTRUM”.

Postanowienia ogólne

§ 2

1. Postanowienia niniejszego regulaminu mają zastosowanie w odniesieniu do wszystkich członków i mieszkańców oraz pracowników Spółdzielni Mieszkaniowej „Centrum” w Ostrołęce i mają na celu zapewnienie ochrony ich prywatności.

2. Regulamin niniejszy określa zasady i tryb przetwarzania danych osobowych i sposoby zabezpieczenia zbiorów danych osobowych będących w posiadaniu Spółdzielni. Określa obowiązki administratora danych osobowych oraz prawa osób, których dane Spółdzielnia przetwarza.

§ 3

1. Użyte w regulaminie określenia oznaczają:

1) Spółdzielnia – Spółdzielnia Mieszkaniowa ‘CENTRUM” w Ostrołęce;

2) dane osobowe – każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby,

3) zbiór danych – każdy posiadający strukturę zestaw danych osobowych dostępnych wg określonych kryteriów, w którym dane są przetwarzane, w szczególności w kartotekach, skorowidzach, księgach, wykazach, rejestrach, systemach informatycznych itp.

4) przetwarzanie danych - wszelkie operacje wykonywane na danych osobowych i ich zbiorach w szczególności; zbieranie, utrwalanie, zmienianie, udostępnianie, przechowywanie, opracowywanie, usuwanie danych osobowych.

5) usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą.

6) Administrator Danych Osobowych (ADO) – podmiot zajmujący się przetwarzaniem danych osobowych. Administratorem Danych Osobowych członków Spółdzielni i jej pracowników jest Spółdzielnia Mieszkaniowa „Centrum” a w jej imieniu Zarząd Spółdzielni.

7) Administrator Bezpieczeństwa Informacji (ABI) – podmiot lub osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, wyznaczona przez ADO.

8) Pracownik – osoba zatrudniona w Spółdzielni na podstawie umowy o pracę lub świadcząca usługę na podstawie umowy cywilno- prawnej.

9) system informatyczny – system przetwarzania informacji wraz z związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje.

§ 4

1. Udostępnienie danych osobowych i informacji stanowiących tajemnicę służbową w Spółdzielni mieszkaniowej odbywa się zgodnie z później opisanymi zasadami:

1) Zarząd Spółdzielni udostępni dane osobowe członka Spółdzielni Walnemu Zgromadzeniu Członków, 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 są udostępnione organom samorządowym Spółdzielni rozpatrującym jego sprawę w postępowaniu wewnątrzspółdzielczym tylko w zakresie mogącym mieć znaczenie dla danej sprawy.
3) Wniosek może dotyczyć jedynie konkretnej osoby, w konkretnej sytuacji i być zgodny z wzorem opublikowanym jako załącznik do rozporządzenia ministra spraw wewnętrznych i administracji w sprawie określenia wzorów wniosków o udostępnienie danych osobowych oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych.
4) Spółdzielnia Mieszkaniowa może odmówić udostępnienia danych osobowych swoich członków i pracowników w przypadkach określonych ustawą o ochronie danych osobowych.
5) Umieszczenie nazwiska członka Spółdzielni na spisie lokatorów na klatce schodowej lub przy instalacji domofonowej jest możliwe po wyrażeniu pisemnej zgody przez członka Spółdzielni.
6) 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.
7) Indywidualni członkowie organów samorządowych 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.

8) Dokumenty udostępnione organom samorządowym nie mogą być wynoszone poza siedzibę Spółdzielni w żadnej postaci, tj. oryginałów, kserokopii czy odpisów.
9) W przypadku podjęcia przez Radę Nadzorczą uchwały o zleceniu badania dokumentów, sporządzenia ekspertyzy lub opinii uprawnionym specjalistom (biegłym), dokumenty wskazane przez Radę Nadzorczą przygotowuje (sporządza kopie) i parafuje upoważniony przez Zarząd pracownik Spółdzielni.
10) 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.

2. Inne zasady:
1) udostępnienie członkom Spółdzielni danych objętych ustawa o ochronie danych, danych i dokumentów stanowiących tajemnicę służbową Spółdzielni, a także innych danych chronionych prawem wynikać może z przepisów odpowiednich ustaw.
2) udostępnienie członkom Spółdzielni informacji chronionych tylko na pisemny wniosek z uzasadnieniem celu ich udostępnienia.

III. OBSZAR PRZETWARZANIA DANYCH

§ 5

1. Zarząd Spółdzielni w drodze decyzji 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 członka Zarządu Spółdzielni.

3. Pomieszczenia, w których są przetwarzane dane osobowe, muszą 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.
5. W przypadku osób, które uzyskały dostęp do pomieszczeń określonych na podstawie upoważnienia Zarządu Spółdzielni, a nie figurują w ewidencji – pracownik składa stosowne oświadczenie.

§ 6

1. Dopuszcza się przetwarzanie danych osobowych na komputerach przenośnych przez użytkowników przeszkolonych w zakresie zachowania szczególnych środków ostrożności oraz korzystania ze środków ochrony kryptograficznej przez administratora bezpieczeństwa informacji, posiadających w rejestrze użytkowników systemu, stosowne upoważnienie.
2. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem Spółdzielni, stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§ 7

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.

§ 8

System informatyczny służący do przetwarzania danych osobowych musi pozwalać na udostępnienie tych danych na piśmie w formie powszechnie zrozumiałej.

1.System informatyczny powinien zapewnić odnotowanie:

1) daty wprowadzenia i modyfikacji danych osobowych,
2) identyfikatora użytkownika systemu wprowadzającego dane,
3) informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione,
4) żądania zaprzestania przetwarzania danych.

2. Administrator systemu informatycznego składa oświadczenie o zapoznanie się z treścią niniejszego regulaminu.

§ 9

Przechowywanie danych

1. Archiwizowane dane nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
2. Urządzenia i systemy informatyczne służące do archiwizowania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
3. Administrator bezpieczeństwa informacji obowiązany jest zabezpieczyć nośniki informacji, wydruki, kopie zapasowe, tak aby uniemożliwić dostęp do nich osobom nieuprawnionym lub przed ich zniszczeniem bądź uszkodzeniem, zgodnie z przepisami rozporządzenia ministra spraw wewnętrznych i administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
4. Kopie awaryjne nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

5. Kopie awaryjne należy okresowo sprawdzać pod kątem ich przydatności do odtwarzania danych w przypadku awarii systemu i bezzwłocznie je usuwać po ustaniu ich użyteczności.

IV. ZBIORY DANYCH OSOBOWYCH

§ 10

Celem zabezpieczenia zbiorów danych osobowych członków 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 wprowadza się poniższe zasady:

1. Spółdzielnia Mieszkaniowa jako administrator danych osobowych przetwarza dane osobowe swoich członków 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) sporządzania list niezbędnych dla obliczania opłat za użytkowanie lokali,
   d) gromadzenia i przetwarzania danych osobowych zawartych w indywidualnych aktach członków Spółdzielni,
   e) wywieszania list/spisów lokatorów na klatkach schodowych i umieszczania nazwisk przy instalacji domofonowej.

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

4. Zarząd Spółdzielni prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych.
5. Ewidencja powinna zawierać:
    a) imię i nazwisko pracownika
    b) stanowisko
    c) zakres, w jakim pracownik został dopuszczony do przetwarzania danych osobowych,
    d) datę wydania upoważnienia,
    e) datę wycofania upoważnienia.
6. Pracownik, który uzyskał upoważnienie do dostępu do zbioru danych osobowych i ich przetwarzania, powinien być zapoznany z przepisami dotyczącymi ochrony danych osobowych.
7. Pracownik Spółdzielni, który uzyskał dostęp do zbioru danych osobowych i ich przetwarzania, zobowiązany jest do złożenia oświadczenia o zachowaniu ich w tajemnicy.
8. Obowiązek ten istnieje również po ustaniu zatrudnienia przy przetwarzaniu danych osobowych.
9. Upoważnienie dostępu do danych osobowych oraz oświadczenie pracownika o zachowaniu w tajemnicy danych osobowych członków Spółdzielni i jej pracowników, dołączone są do akt osobowych pracownika.
10. Indywidualny zakres czynności pracownika dopuszczonego 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 danych.

§ 11

1. Sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych z uwzględnieniem wymogów bezpieczeństwa informacji określa instrukcja, która powinna zawierać:
    1) określenie sposobu przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności,

2) określenie sposobu rejestrowania i wyrejestrowania użytkownika oraz wskazanie osoby odpowiedzialnej za te czynności,
3) procedury rozpoczęcia i zakończenia pracy,
4) metodę i częstotliwość tworzenia kopii awaryjnych,
5) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
6) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych.

2. Odpowiedzialnym za przygotowanie i wdrożenie instrukcji jest ADO.

V. OCHRONA DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM

§ 12

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

§ 13

1. Pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym administrator 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 powinien utrzymywać w tajemnicy, także po upływie jego ważności.
7. Bezpośredni dostęp do systemu informatycznego zawierającego dane osobowe może nastąpić wyłącznie po podaniu identyfikatora i hasła.

§ 14

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

§ 15

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 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, jego przyczynach i skutkach oraz podjętych działaniach korygujących system.

§ 16

Administrator bezpieczeństwa informacji obowiązany jest zabezpieczyć nośnik informacji, wydruki, kopie zastępcze tak, aby uniemożliwić dostęp do nich osobom nieuprawnionym lub przed ich uszkodzeniem lub zniszczeniem, zgodnie z przepisami rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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 r. nr 100, poz. 1024 ze zm.).

§ 17

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,
- data wydania upoważnienia,

- data utraty upoważnienia,
- indywidualny identyfikator pracownika.

VI. PRZEPISY KOŃCOWE

§ 18

1. Niniejszy Regulamin stosuje się do: członków organów samorządowych, tj. Rady Nadzorczej i Zarządu Spółdzielni oraz upoważnionych pracowników Spółdzielni.
2. Integralną część Regulaminu stanowią wzory oświadczeń (załączniki nr 1, 2, 3) o zachowaniu tajemnicy danych osobowych, tajemnicy służbowej i innych danych prawnie chronionych, w tym wzór oświadczenia członka organu samorządowego.
3. Regulamin został zatwierdzony Uchwałą Nr 4/17 Rady Nadzorczej w dniu 27 lutego 2017r. i wchodzi w życie z dniem podjęcia.