Załącznik

do Zarządzenia Zarządu SM w Gubinie Nr 9 z dn. 02.10.2017 r.

REGULAMIN OCHRONY DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ W GUBINIE

REGULAMIN OCHRONY DANYCH OSOBOWYCH I INFORMACJI STANOWIĄCYCH TAJEMNICE PRAWNIE CHRONIONE W SPÓŁDZIELNI MIESZKANIOWEJ W GUBINIE.

I. POSTANOWIENIA OGÓLNE

§ 1.1. Ochrona danych osobowych w Spółdzielni Mieszkaniowej w Gubinie ma na celu zapewnienie każdemu członkowi Spółdzielni, mieszkańcom i jej pracownikom ochronę ich prywatności.

2. Ochrona informacji stanowiących tajemnicę służbową w Spółdzielni ma na celu ich zabezpieczenie przed nieuprawnionym ujawnianiem, które może spowodować szkodę dla prawnie chronionych interesów Spółdzielni innych osób w tym jednostek organizacyjnych – podmiotów gospodarczych.
3. Regulamin niniejszy określa zasady i tryb przetwarzania danych osobowych i sposobu zabezpieczenia zbiorów danych osobowych będących w posiadaniu Spółdzielni, a także określa obowiązki Administratora Danych Osobowych, których dane Spółdzielnia przetwarza.
4. Regulamin określa również zakres ochrony informacji stanowiących tajemnicę służbową, w tym handlową Spółdzielni, do której dostęp mają pracownicy i członkowie organów samorządowych Spółdzielni, w związku z czynnościami służbowymi, pełnioną funkcją lub w związku z działalnością społeczną.

§ 2. Podstawę prawną niniejszego regulaminu stanowią przepisy:

- ustawy z dnia 29.08.1997r. o ochronie danych osobowych (j.t. Dz. U. 2016, poz.922);
- ustawy z dnia 16.04.1993r. o zwalczaniu nieuczciwej konkurencji (j.t. Dz. U. 2003 Nr 153, poz. 1503);
- ustawy z dnia 06.06.1997r. kodeks karny – (j.t. Dz. U. 2016, poz. 1137));
- ustawy z dnia 23.04.1964r. kodeks cywilny (Dz. U. 2014, poz. 121)
- ustawy z dnia 26.06.1974r. kodeks pracy (j.t. Dz. U. 2014, poz. 1502)
- ustawy z dnia 16.09.1982r. – Prawo spółdzielcze (j.t. Dz. U. 2016, poz.21);
- ustawy z dnia 15.12.2000r. – o spółdzielniach mieszkaniowych (j.t. Dz. U.2013, poz.1222);
- rozporządzenia 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 z 2004r. Nr 100, poz.1024)

- dyrektywy 95/46/EC Parlamentu Europejskiego I Rady z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.

§ 3. Przez użyte w treści regulaminu sformułowanie należy rozumieć:

1. Spółdzielnia – Spółdzielnia Mieszkaniowa w Gubinie,
2. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej ,
3. Zbiór danych – każdy posiadający strukturę zestaw danych osobowych o charakterze osobowym, dostępnych wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie (w szczególności: w kartoteki, skorowidze, księgi, wykazy, rejestry, systemy informatyczne, itp.),
4. Przetwarzanie danych – wszystkie operacje wykonywane na danych osobowych i ich zbiorach, w szczególności: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych,
5. Usuwanie danych – zniszczenie danych osobowych lub 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, a w jej imieniu Zarząd Spółdzielni,
7. Administrator Bezpieczeństwa Informacji (ABI) – osoba odpowiedzialna za bezpieczeństwo przetwarzanych danych osobowych, wyznaczona przez Administratora Danych Osobowych,
8. System informatyczny – system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje,
9. Tajemnica służbowa – informacje dotyczące działalności inwestycyjnej, prowadzonej działalności gospodarczej i innej, stanowiące tajemnicę przedsiębiorstwa Spółdzielni oraz informacje o kontraktach Spółdzielni w związku z czynnościami służbowymi, albo wykonywaniem prac zleconych również społecznych, której ujawnienie mogłoby narazić na szkodę interes Spółdzielni lub prawnie chroniony interes innych osób, albo jednostek organizacyjnych – podmiotów gospodarczych.

§ 4. Celem zabezpieczenia zbiorów danych osobowych członków Spółdzielni, jej pracowników i ich kontrahentów, a także zabezpieczenia ich przetwarzania, jest uniemożliwienie dostępu do zbioru danych osobom nieuprawnionym, bądź zbierania ich przez osobę nieuprawnioną oraz zabezpieczenia danych przed ich uszkodzeniem lub zniszczeniem.

§ 5.1. Spółdzielnia jako Administrator Danych Osobowych przetwarza dane osobowe swoich członków i mieszkańców dla realizacji celów statutowych w zakresie:

a) Prowadzenia rejestru członków i lokatorów,
b) Prowadzenia rejestru lokali, dla których zostały założone księgi wieczyste z adnotacją o ustanowionych hipotekach,
c) Listy przydziałów mieszkań,

d) Sporządzania list niezbędnych dla obliczania opłat za używanie lokali,

e) 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.

§ 6.1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mogą mieć wyłącznie pracownicy, którzy uzyskali pisemne upoważnienie wydane przez Zarząd Spółdzielni

2. Zarząd Spółdzielni prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych oraz wydanych upoważnień.

3. Ewidencja, o której mowa w ust. 2, 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) identyfikator, w przypadku przetwarzania danych osobowych w systemie informatycznym.

4. Pracownik, który uzyskał upoważnienie dostępu do zbioru danych osobowych i ich przetwarzania, powinien być zapoznany z przepisami dotyczącymi ochrony danych osobowych.

5. Pracownik Spółdzielni, który uzyskał dostęp do zbioru danych osobowych i ich przetwarzania, zobowiązany jest do złożenia oświadczenia o zachowaniu ich w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia przy przetwarzaniu danych osobowych.

6. Upoważnienie, o którym mowa w ust. 1 oraz oświadczenie pracownika o zachowaniu w tajemnicy danych osobowych członków Spółdzielni i jej pracowników dołączone jest do akt osobowych pracownika.

7. 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 tych danych.

§ 7.1. Dane osobowe członków Spółdzielni i jej pracowników są przechowywane w zabezpieczonych pomieszczeniach.

2. Do pomieszczeń, o których mowa w ust. 1, mogą mieć dostęp jedynie pracownicy Spółdzielni posiadający upoważnienie do przetwarzania danych osobowych.

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

4. Zabezpieczeniu podlegają także dane dotyczące kontrahentów Spółdzielni. Sposób zabezpieczenia określa Zarząd Spółdzielni.

II. OCHRONA DANYCH OSOBOWYCH I ICH PRZETWARZANIA W SYSTEMIE INFORMATYCZNYM

§ 8.1. Przy obsłudze systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania danych, mogą być zatrudnieni wyłącznie pracownicy posiadający upoważnienia wydane przez Zarząd Spółdzielni.

2. Zarząd Spółdzielni wyznacza Administratora Bezpieczeństwa Informacji lub inną osobę odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w systemie informatycznym.

3. Administrator Bezpieczeństwa Informacji lub inna wyznaczona osoba odpowiedzialny jest za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz podejmowanie odpowiednich działań w przypadkach wykrycia naruszeń w systemie zabezpieczeń.

§ 9.1. Pracownikowi Spółdzielni zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym Administrator Bezpieczeństwa Informacji lub inna wyznaczona osoba 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 co 90 dni.

5. Hasło powinno zawierać minimum 9 znaków, w tym litery duże i małe, cyfry oraz znaki specjalne.

6. Hasło przydzielone pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych pracownik powinien użytkować w tajemnicy, także po upływie jego ważności.

7. Bezpośredni dostęp do systemu informatycznego zawierającego dane osobowe może nastąpić wyłącznie po podaniu identyfikatora i hasła.

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

§ 10.1. Pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie informatycznym obowiązany jest niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub Administratora Danych Osobowych, gdy:

a) stwierdzi naruszenie bezpieczeństwa systemu informatycznego,
b) 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 lub inna wyznaczona przez ADO osoba 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 korekt w systemie informatycznym polegającym na zabezpieczeniu systemu przed ponownym jego naruszeniem,
e) powiadomić Zarząd Spółdzielni o naruszeniu systemu informatycznego, jego przyczynach i skutkach oraz podjętych działaniach korygujących system.

§ 11. Administrator Bezpieczeństwa Informacji prowadzi rejestr pracowników – użytkowników systemu informatycznego, zawierający:

a) imię i nazwisko pracownika,
b) stanowisko,
c) zakres, w jakim pracownik został dopuszczony do przetwarzania danych osobowych w systemie informatycznym,
d) datę wydania upoważnienia,
e) datę utraty upoważnienia,
f) indywidualny identyfikator pracownika.

§ 12. System informatyczny powinien zapewniać odnotowanie:

a) daty wprowadzenia i modyfikacji danych osobowych,
b) identyfikatora użytkownika systemu wprowadzającego dane,
c) informację, komu, kiedy i w jakim zakresie dane zostały udostępnione,
d) żądania zaprzestania przetwarzania danych po jego uwzględnieniu.

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

2. Dane przedstawione w formie pisemnej powinny zawierać informacje określone w § 12.

§ 14. Zarząd Spółdzielni w drodze zarządzenia określi pomieszczenia lub ich części, tworząc obszar, w którym przetwarzane są dane osobowe w systemie informatycznym.

1. 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.

2. 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.

3. W pomieszczeniach, w których przebywają osoby postronne, monitory komputerów powinny być ustawione w taki sposób, żeby uniemożliwić im wgląd w dane osobowe.

§ 15. 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.

§ 16.1. 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, o którym mowa w § 14 ust. 1, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§ 17. 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 z dnia 29 kwietnia 2004r. 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. 2004, poz. 1024 ze zm.).

§ 18.1. Kopie awaryjne nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

2. Kopie awaryjne należy:

a) okresowo sprawdzić pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
b) bezzwłocznie usunąć po ustaniu ich użyteczności.

§ 19. Szczegółowe zasady ochrony danych osobowych i ich przetwarzania w systemie informatycznym są zawarte w „Polityce Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym".

III. OCHRONA TAJEMNICY SŁUŻBOWEJ I INFORMACJI PRAWNIE CHRONIONEJ W SPÓŁDZIELNI MIESZKANIOWEJ W GUBINIE

§ 20.1. 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 Mieszkaniowej w Gubinie 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, osiągane 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.

IV. UDOSTĘPNIANIE DANYCH OSOBOWYCH I INFORMACJI STANOWIĄCYCH TAJEMNICĘ SŁUŻBOWĄ W SPÓŁDZIELNI MIESZKANIOWEJ W GUBINIE

§ 21.1. Zarząd Spółdzielni udostępni dane osobowe członka Spółdzielni 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. Dokumenty udostępnione organom samorządowym nie mogą być wynoszone poza siedzibę Spółdzielni w żadnej postaci tj. oryginałów, kserokopii czy odpisów.

4. 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.

§ 22.1. Udostępnienie danych osobowych przetwarzanych przez Spółdzielnię osobom fizycznym lub instytucjom publicznym może nastąpić w trybie art. 31 §1 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych w przypadkach określonych w ustawie.

2. Tryb określony w ust. 1, Administrator Danych Osobowych uruchamia na pisemnie umotywowany wniosek.

3. Spółdzielnia Mieszkaniowa może odmówić udostępnienia danych osobowych swoich członków i pracowników w przypadkach określonych ustawą o ochronie danych osobowych.

4. Umieszczenie nazwiska członka Spółdzielni na liście lokatorów lub przy instalacji domofonowej jest możliwe po wyrażeniu pisemnej zgody przez członka Spółdzielni.

§ 23.1. Osoba, której dane przetwarzane są przez Spółdzielnię ma prawo do informacji o:

a) sposobie przetwarzania danych osobowych (ręczne przetwarzanie danych, metody informatyczne, w tym sieci komputerowe),
b) treści danych,
c) sposobie udostępnienia danych osobowych oraz odbiorcach lub kategorii odbiorców danych.

2. Informacji, o których mowa w ust. 1, Zarząd Spółdzielni jest zobowiązany udzielić w terminie 30 dni od daty otrzymania wniosku.

V. PRZEPISY KOŃCOWE

§ 24. Niniejszy Regulamin obowiązuje: członków organów samorządowych tj. Radę Nadzorczą i Zarząd Spółdzielni oraz upoważnionych pracowników Spółdzielni.

1. Regulamin został zatwierdzony Zarządzeniem Zarządu SM w Gubinie Nr 9 z dnia 02.10.2017 r.

i wchodzi w życie z dniem podjęcia.