Załącznik do uchwały Zarządu SBM „Kwitnąca”

nr 1/V/2018 z dnia 25.05.2018 r.

**Polityka bezpieczeństwa danych osobowych**

**w Spółdzielni Budowlano-Mieszkaniowej „Kwitnąca”**

§ 1

**Podstawa prawna**

Polityka bezpieczeństwa uwzględnia wymagania prawne dotyczące zasad przetwarzania i zabezpieczenia danych osobowych w szczególności wynikające z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO) oraz Ustawy z dnia 10 maja 2018 r. o Ochronie Danych Osobowych.

§ 2

**Polityka bezpieczeństwa danych osobowych - cele**

1. Polityka bezpieczeństwa danych osobowych ma na celu wdrożenie i utrzymanie odpowiednich środków technicznych i organizacyjnych dla zapewnienia bezpieczeństwa danych osobowych i ich przetwarzania zgodnie z obowiązującymi przepisami.

2. Wdrożenie Polityki bezpieczeństwa danych związane jest z maksymalnym ograniczeniem ryzyka nieuprawnionego przetwarzania lub utraty danych osobowych a w szczególności w celu ochrony interesów osób, których dane dotyczą.

3. Polityka ochrony danych osobowych określa tryb i zasady przetwarzania danych osobowych i sposobu zabezpieczenia zbiorów danych osobowych, będących w posiadaniu Spółdzielni, a także określa obowiązki Administratora danych.

4. SBM „Kwitnąca”, realizując politykę bezpieczeństwa w zakresie danych osobowych, dąży do zapewnienia by dane osobowe były:

* przetwarzane zgodnie z prawem,
* zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
* poprawne i adekwatne do celów w jakich są przetwarzane,
* przechowywane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 3

**Definicje**

1. Administrator danych (lub: Administrator) – Spółdzielnia Budowlano - Mieszkaniowa „Kwitnąca” w Warszawie, w której imieniu działają w tym zakresie członkowie Zarządu.

2. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

3. Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej (dokumentowej) oraz w systemach informatycznych.

4. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

5. Użytkownik – osoba upoważniona przez Administratora danych do przetwarzania danych osobowych.

6. Zbiór danych – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów.

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

8. Naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

9. Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

10. Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się Dane osobowe.

11. Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie przetwarzania danych osobowych w takim systemie.

12. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie.

§ 4

**Dane osobowe zbierane i przetwarzane w SBM „Kwitnąca”**

1. Spółdzielnia przetwarza dane osobowe swoich członków, osób posiadających tytuły prawne do lokali w budynkach do niej należących i osób w nich zamieszkujących dla realizacji celów statutowych.

2. Zakres przetwarzania danych obejmuje:

* prowadzenie rejestru członków zawierającego imię i nazwisko, adres lokalu, numer członkowski, datę powstania członkostwa, datę i przyczynę ustania, podstawę nabycia członkostwa;
* prowadzenie rejestru lokali, dla których zostały założone księgi wieczyste (w tym adnotacje o hipotekach);
* gromadzenie i przetwarzanie danych zawartych w indywidualnych aktach członków spółdzielni oraz aktach osób posiadających tytuł prawny do lokalu;
* gromadzenie danych niezbędnych do obliczenia opłat za używanie lokali;
* prowadzenie indywidualnych rozliczeń pomiędzy użytkownikami lokali a spółdzielnią;
* prowadzenie procedur windykacyjnych w przypadku zaległości w opłatach za lokal.

3. 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.

4. Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych;

5. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 2 do niniejszej Polityki.

6. Zabronione jest zbieranie i przetwarzanie danych ujawniających pochodzenie rasowe lub etniczne, przekonania religijne lub światopoglądowe, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, nałogach lub życiu seksualnym.

7. Dane dotyczące orzeczeń o ukaraniu, mandatach karnych, a także inne orzeczenia wydane w postępowaniu administracyjnym lub sądowym mogą być przetwarzane wyłącznie w celu realizacji praw i obowiązków spółdzielni wynikających z tych orzeczeń.

§ 5

**Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem danych osobowych**

1. Dostęp do zbioru danych osobowych oraz ich przetwarzanie mogą mieć wyłącznie pracownicy i organy statutowe spółdzielni, którzy otrzymali pisemne upoważnienie wydane przez administratora.

2. Osoby upoważnione do dostępu do danych osobowych zobowiązane są do zapoznania się z niniejszą polityką bezpieczeństwa danych osobowych i potwierdzenie tego własnoręcznym podpisem na kopii upoważnienia, przechowywanej w aktach osobowych lub dokumentach Rady Nadzorczej.

3. Administrator prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych oraz wydanych upoważnień - wzór stanowi Załącznik nr 3.

4. Ewidencja powinna zawierać:

- imię nazwisko, PESEL osoby upoważnionej,

- stanowisko,

- zakres dopuszczenia do przetwarzania danych osobowych.

5. Osoba, która uzyskała dostęp do zbioru danych osobowych i ich przetwarzania zobowiązana jest do złożenia oświadczenia o zachowaniu ich w tajemnicy – wzór oświadczenia stanowi Załącznik nr 4.

§ 6

**Klauzula informacyjna**

1. Obowiązek informacyjny wobec osób, których dotyczy przetwarzanie danych osobowych realizowany jest poprzez zapoznanie ich z klauzulą informacyjną stanowiącą Załącznik nr 1 do niniejszej Polityki bezpieczeństwa danych osobowych.

2. Zapoznanie z klauzulą informacyjnąrealizuje się poprzez umieszczenie treści klauzuli w gablotach informacyjnych oraz na stronie internetowej Spółdzielni.

§ 7

**Środki techniczne i organizacyjne dla zapewnienia ochrony danych osobowych**

1. Administrator danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych osobowych.

2. Zastosowane środki ochrony (techniczne i organizacyjne) obejmują m.in.:

* ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe jedynie dla osób upoważnionych (użytkowników). Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie użytkownika i pod jego nadzorem;
* zamykanie pomieszczeń tworzących obszar przetwarzania danych osobowych na czas nieobecności pracowników Administratora w sposób uniemożliwiający dostęp do nich osób trzecich (tzw. polityka kluczy - polegająca na zamykaniu na klucz lub innego rodzaju równoważne zabezpieczenie pomieszczeń, w których znajdują się bądź są przetwarzane dane osobowe – w każdym przypadku nieobecności użytkownika;
* stosowanie polityki czystego biurka, polegającej na tym, że wszelkie dokumenty zawierające dane osobowe nie mogą pozostawać na stanowisku pracy w czasie nieobecności (choćby chwilowej) użytkownika. W przypadku takiej nieobecności użytkownik ma obowiązek wszelkie dokumenty zabezpieczyć w sposób uniemożliwiający zapoznanie się z nimi osobom trzecim (np. poprzez umieszczenie tychże w szafach);
* stosowanie polityki czystego ekranu, polegającej na tym, że w przypadku odejścia od stanowiska pracy wyposażonego w urządzenia posiadające dostęp do elektronicznych zbiorów danych (danych osobowych) użytkownik zobowiązany jest do każdorazowego wylogowania się lub zablokowania dostępu do urządzenia w taki sposób, aby niemożliwym było uzyskanie dostępu przez osobę nieuprawnioną;
* wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe;
* ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu tzw. „firewall’a”;
* ustawienie monitorów komputerów w taki sposób aby uniemożliwić osobom postronnym wgląd w dane osobowe;
* dane osobowe gromadzone w teczkach i segregatorach przechowywane są w zamykanych na klucz szafach.

§ 8

**Ochrona danych osobowych w systemie informatycznym**

**I. dostęp do systemu informatycznego**

1. Przy obsłudze systemu informatycznego i komputerowego systemu księgowego oraz obsłudze urządzeń wchodzących w jego skład mogą być zatrudnione osoby posiadające upoważnienie wydane przez administratora (lub z którymi podpisana jest umowa o powierzeniu przetwarzania danych).

2. Pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym administrator danych osobowych lub osoba zarządzająca siecią informatyczną w spółdzielni przydziela odrębny identyfikator i hasło.

3. Hasło przydzielone podczas przyznawania uprawnień powinno być zmienione na indywidualne podczas pierwszego logowania się użytkownika w systemie.

4. Dostęp do systemu informatycznego i danych osobowych w nim zawartych może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

5. Stosowane hasła:

* muszą liczyć co najmniej 8 znaków składających się z małych i dużych liter oraz cyfr,
* nie mogą składać się z ogólnie dostępnych informacji o użytkowniku, w szczególności z imion, nazwiska, daty urodzenia, liczb będących numerem PESEL, telefonu itp. Dotyczących także osób z najbliższej rodziny użytkownika.

6. Pracownik lub upoważniony użytkownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

7. Identyfikator i hasło osoby, która utraciła uprawnienia do dostępu do danych osobowych jest niezwłocznie blokowane w systemie informatycznym przez administratora lub osobę zarządzającą siecią informatyczną spółdzielni.

8. Identyfikator użytkownika nie może być zmieniany bez wyraźnej przyczyny i nie może być przydzielony innej osobie po wyrejestrowaniu użytkownika z systemu informatycznego (odebraniu uprawnień).

9. Pracownicy/użytkownicy są odpowiedzialni za zachowanie poufności swoich identyfikatorów i haseł także po upływie ich ważności.

**II. Praca z danymi w systemie informatycznym**

1. Rozpoczęcie pracy w systemie komputerowym wymaga zalogowania się do systemu przy użyciu indywidualnego identyfikatora oraz hasła dostępu.

2. Przed opuszczeniem stanowiska pracy należy zablokować stację roboczą w taki sposób aby niemożliwe było uzyskanie dostępu do niej przez osobę nieuprawnioną lub wylogować się z oprogramowania i systemu operacyjnego.

3. W trakcie pracy w przypadku konieczności opuszczenia stanowiska komputerowego należy za każdym razem dopilnować, aby na ekranie nie były wyświetlane dane osobowe.

4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wylogować się z systemu operacyjnego i wykonać zamknięcie systemu.

5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania systemu operacyjnego.

**III. utrzymanie systemu informatycznego Spółdzielni**

1. Osoba zatrudniona do obsługi, konserwacji i utrzymania systemu informatycznego w Spółdzielni jest jednocześnie osobą zarządzającą siecią informatyczną spółdzielni.

2. Osoba zarządzająca siecią informatyczną Spółdzielni otrzymuje uprawnienia do dostępu do danych osobowych na podstawie umowy powierzenia danych lub pisemnego upoważnienia wydanego przez Administratora.

3. Osoba ta odpowiedzialna jest za:

* dokonywanie przeglądu, napraw, konserwacji i likwidacji sprzętu komputerowego, na którym zapisane są dane osobowe, a w przypadku realizacji tych zadań przez podmiot zewnętrzny – nadzór nad realizacją w/w zadań,
* przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
* zabezpieczenie systemu informatycznego,
* podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Spółdzielni w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych,
* podejmowanie działań w przypadku naruszeń w systemie zabezpieczeń, - podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
* tworzenie kopii zapasowych,
* współpracę dotyczącą systemu informatycznego Spółdzielni z firmą obsługującą program księgowy Spółdzielni.

**IV. Zabezpieczenie systemu**

1. System informatyczny musi być zabezpieczony przed działaniem programów, których celem jest uzyskanie nieuprawionego dostępu do systemu oraz przed działaniami inicjowanymi z sieci zewnętrznej.

2. Zabezpieczenie obejmuje m.in.:

* zabezpieczenie programem antywirusowym,
* zabezpieczenie programem typu „firewall”,
* szyfrowanie nośników danych,
* zabezpieczenie sieci radiowej uwierzytelnieniem kluczem WPA-2,
* zabezpieczenie przed skutkami awarii zasilania w postaci urządzenia typu UPS,
* szyfrowanie danych.

3. oprogramowanie antywirusowe z włączoną ochroną antywirusową i antyspyware musi być zainstalowane na każdym stanowisku komputerowym.

4. Zabronione jest samowolne instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek urządzeń do systemu informatycznego niezatwierdzonych przez osobę zarządzającą siecią informatyczną Spółdzielni.

5. Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zasilane energią elektryczną, powinny być zabezpieczone przed utratą danych, spowodowaną awarią zasilania.

**V. Kopie zapasowe**

1. Za systematyczne sporządzanie kopii zapasowych odpowiada osoba zarządzającą siecią informatyczną Spółdzielni, nadzorowana bezpośrednio przez Administratora danych.

2. Kopie bezpieczeństwa wykonywane są na koniec każdego miesiąca kalendarzowego.

3. Kopie bezpieczeństwa wykonywane są na dyskach zewnętrznych przechowywanych w biurze Spółdzielni w zamykanej na klucz szafie w pomieszczeniu księgowości.

§ 9

**Powierzenie przetwarzania danych osobowych**

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO. Wzór takiej umowy określa Załącznik nr 5 do niniejszej Polityki.

2. Dane osobowe członka spółdzielni oraz użytkowników lokali mogą być udostępnione Radzie Nadzorczej Spółdzielni w związku ze sprawowaniem funkcji kontrolnych na podstawie ustawy prawo spółdzielcze, ustawy o spółdzielniach mieszkaniowych oraz statutu Spółdzielni. Wzór upoważnienia dla członka Rady Nadzorczej stanowi Załącznik nr 6 do niniejszej Polityki.

§ 10

**Naruszenie ochrony danych osobowych**

1. Za naruszenie ochrony danych osobowych lub próbę takiego naruszenia uważa się w szczególności:

* naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe udostępnianie lub umożliwienie udostępniania danych osobowych osobom lub podmiotom do tego nieupoważnionym;
* zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
* niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
* przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania; spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;
* naruszenie praw osób, których dane osobowe są przetwarzane.

2. W przypadku stwierdzenia możliwości naruszenia zasad ochrony danych osobowych użytkownik zobowiązany jest do podjęcia wszelkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora danych.

3. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

4. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator niezwłocznie zawiadamia o incydencie także osobę, której dane dotyczą.

5. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu – nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

6. Administrator po ustaleniu zakresu, przyczyn i skutków naruszenia ochrony danych osobowych podejmie wszelkie niezbędne środki do przywrócenia stanu sprzed naruszenia oraz podejmie działania uniemożliwiające podobne naruszenia w przyszłości.

7. Administrator dokumentuje wszelkie incydenty naruszenia ochrony danych osobowych (zgodnie z przepisem art. 33 ust. 5 RODO), w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

§ 10

**Postanowienia końcowe**

1. Czas przechowywania danych osobowych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane (niszczone);

2. Osoba, której dane przetwarzane są przez Spółdzielnię ma prawo do:

* informacji o sposobie przetwarzania danych
* treści danych
* sposobie udostępnienia danych osobowych oraz odbiorcach lub kategorii odbiorców danych,
* żądania uzupełnienia , uaktualnienia i sprostowania danych osobowych.

2. Niniejsza Polityka bezpieczeństwa wchodzi w życie z dniem 25.05.2018 r. tj. z chwilą podjęcia przez Zarząd uchwały o jej wprowadzeniu.

Załączniki:

Załącznik nr 1 – klauzula informacyjna

Załącznik nr 2 – wzór rejestru czynności przetwarzania danych

Załącznik nr 3 – wzór ewidencji osób zatrudnionych przy przetwarzaniu danych oraz wydanych upoważnień

Załącznik nr 4 – wzór oświadczenia o zachowaniu danych osobowych w tajemnicy

Załącznik nr 5 – wzór umowy Powierzenia przetwarzania danych osobowych

Załącznik nr 6 - wzór upoważnienia dla członka Rady Nadzorczej