

**Załącznik do Uchwały Nr 7/2018 z dnia 25.09.2018 r.
Zarządu Spółdzielni Mieszkaniowej „CENTRUM” w
Otwocku**

**INSTRUKCJA OCHRONY DANYCH OSOBOWYCH
W SPÓŁDZIELNI MIESZKANIOWEJ „CENTRUM” W OTWOCKU**

I. POSTANOWIENIA OGÓLNE

§ 1

1. Podstawa prawna: rozporządzenie Parlamentu Europejskiego i Rady (EU) 216/679 z dnia 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 (ogólne rozporządzenie o ochronie danych), zwane dalej „RODO”.

2. Instrukcja określa zasady ochrony danych osobowych w Spółdzielni Mieszkaniowej „CENTRUM w Otwocku zwanej dalej „Spółdzielnią”, obowiązki Administratora oraz podmiotów przetwarzających.

§ 2

1. Przez użyte w Instrukcji określenia należy rozumieć:

1) dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,

2) zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, w którym dane są przetwarzane w szczególności:

- w kartotekach,
- w skorowidzach,
- w księgach,
- w wykazach,
- w rejestrach,
- w systemach informatycznych,

3) przetwarzanie danych – wszelkie operacje wykonywane na danych osobowych i zestawach danych osobowych w szczególności takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

4) Administrator - Spółdzielnia Mieszkaniowa „CENTRUM” w Otwocku reprezentowana przez Zarząd,

5) administrator bezpieczeństwa informacji – osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, wyznaczona przez Administratora,

- 6) system informatyczny – to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
- 7) Spółdzielnia – Spółdzielnia Mieszkaniowa „CENTRUM” w Otwocku.

§ 3

Ochrona danych osobowych w Spółdzielni wykonywana jest z uwzględnieniem zasady minimalizacji danych oraz stosowania niezbędnych zabezpieczeń przy przetwarzaniu danych oraz ochrony danych osób, których dane dotyczą.

§ 4

1. Administrator przetwarza dane osobowe dla realizacji celów ustawowych i statutowych w szczególności w zakresie:

- 1) prowadzenia rejestru członków,
- 2) prowadzenia rejestru lokali (dla spółdzielczych własnościowych praw do lokali), dla których zostały założone oddzielne księgi wieczyste,
- 3) prowadzenia list, kartotek i urządzeń księgowych niezbędnych dla obliczania opłat za używanie lokali,
- 4) przetwarzania danych osobowych zawartych w indywidualnych aktach,
- 5) zwoływania i obsługi organów Spółdzielni,
- 6) rozpatrywania skarg, wniosków i postulatów członków, mieszkańców i innych osób fizycznych,
- 7) wywieszania spisu mieszkańców domu i umieszczania nazwisk przy instalacji domofonowej,
- 8) prowadzenia działalności gospodarczej dla dobra Spółdzielni,
- 9) windykacji należności Spółdzielni.

2. Administrator przetwarza dane osobowe:

- zgodnie z art. 6 ust. 1 pkt c RODO w celu wypełnienia obowiązków prawnych nałożonych na podstawie ustawy z dnia 16 września 1982 r. Prawo spółdzielcze i ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (ust. 1 pkt 1-3,5,8),
- zgodnie z art. 6 ust. 1 pkt a RODO po wyrażeniu zgody przez osobę, której dane dotyczą w jednym lub większej liczbie celów (ust.1 pkt 4,6 i 7),
- zgodnie z art. 6 ust. 1 pkt b RODO w celu wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (ust. 1 pkt 4, 8) ,
- zgodnie z art. 6 ust. 1 pkt f RODO w celach wynikających z prawnie uzasadnionych interesów Spółdzielni lub osoby trzeciej (ust. 1 pkt 3, 8 i 9).

3. Administrator przetwarza dane osobowe swoich pracowników zawarte w aktach osobowych w zakresie określonym przepisami Kodeksu pracy i innych ustaw.
4. Prawo do przeglądania rejestru członków przysługuje członkom Spółdzielni, jego małżonkom, wierzycielom członka lub Spółdzielni. W tym wypadku nie stosuje się przepisu ust.1 § 5.
5. Prawo do przeglądania rejestru lokali (dla spółdzielczych własnościowych praw do lokali), dla których zostały założone oddzielne księgi wieczyste, przysługuje każdej osobie. W tym wypadku nie stosuje się przepisu ust.1 § 5.
6. W razie przeglądania rejestrów określonych w ust. 4 i 5 należy odnotować dane osobowe osoby, której udostępniono rejestr (imię, nazwisko, miejsce zamieszkania, ewentualny interes prawny).
7. Akta indywidualne(tzw. członkowskie, lokalowe, podręczne) nie mogą być udostępniane do przetwarzania osobom trzecim, chyba że zachodzą przesłanki określone w art. 9 ust. 2 RODO. W każdej takiej sprawie podjęcie decyzji jest zastrzeżone wyłącznie dla Administratora.

§ 5

1. Dostęp do zbioru danych osobowych oraz do ich przetwarzania mogą mieć wyłącznie osoby, które uzyskały pisemne upoważnienie wydane przez Administratora, z zastrzeżeniem wyjątków określonych w niniejszej Instrukcji.
2. Administrator prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych.
3. Ewidencja, o której mowa w ust. 2 powinna zawierać:
 - imię i nazwisko,
 - stanowisko,
 - zakres, w jakim pracownik został dopuszczony do przetwarzania danych osobowych,
 - datę wydania upoważnienia,
 - identyfikator w przypadku przetwarzania danych osobowych w systemie informatycznym.
4. Pracownik, który uzyskał upoważnienie do 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. 2 oraz oświadczenie pracownika o zachowaniu danych osobowych składa się 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.
8. Przepisy ust. 1-7 stosuje się odpowiednio do umów zawieranych przez Spółdzielnię z kontrahentami, z których wynika możliwość dostępu do zbioru danych osobowych i ich przetwarzania.

§ 6

1. Dane osobowe są przetwarzane w Spółdzielni, w wydzielonych pomieszczeniach określonych przez Administratora.
2. Do pomieszczeń, o których mowa w ust. 1 mogą mieć dostęp jedynie pracownicy Spółdzielni posiadający upoważnienie Administratora.
3. Pomieszczenia, w których przetwarzane są dane osobowe, są zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych osobowych.

II. OCHRONA DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM

§ 7

1. Przy obsłudze systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych mogą być zatrudnieni wyłącznie pracownicy posiadający upoważnienie wydane przez Administratora.
2. Administrator może wyznaczyć pracownika odpowiedzialnego za bezpieczeństwo danych osobowych gromadzonych i przetwarzanych w systemie informatycznym.
3. Pracownik ten 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.
4. Administratorem bezpieczeństwa danych może być:
 - 1) pracownik Spółdzielni zatrudniony na podstawie umowy o pracę,
 - 2) podmiot, posiadający uprawnienia do świadczenia usług w zakresie wymaganym ustawą, z którym Spółdzielnia zawarła umowę cywilnoprawną, a przedmiot umowy obejmuje zakres obowiązków wynikający z RODO.
5. W razie niewyznaczenia pracownika jego obowiązki wykonuje Administrator.

§ 8

1. Pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym Spółdzielni przydziela się 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 30 dni.
5. Hasło powinno zawierać co najmniej 8 znaków w tym 1 duża litera, 1 mała i 1 cyfra.
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.
8. Identyfikator osoby, która utraciła uprawnienia dostępu do systemu informatycznego zawierającego dane osobowe, należy natychmiast wyrejestrować z systemu i unieważnić jej hasło.
9. Spółdzielnia przy przetwarzaniu danych w systemie informatycznym stosuje przepisy właściwe dla poziomu wykonywanych operacji, z uwzględnieniem przepisu § 3.

§ 9

1. Pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie informatycznym obowiązany jest niezwłocznie powiadomić Administratora gdy:
 - stwierdzi naruszenie zabezpieczenia systemu informatycznego,
 - stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakości komunikacji sieci mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. Administrator po stwierdzeniu naruszenia systemu informatycznego ma obowiązek:
 - zabezpieczyć ślady pozwalające na określenie przyczyny naruszenia systemu informatycznego,
 - przeanalizować i określić skutki naruszenia systemu informatycznego,
 - określić czynniki, które spowodowały naruszenie systemu informatycznego,
 - dokonać niezbędnych korekt w systemie informatycznym polegających na zabezpieczeniu systemu przed ponownym jego naruszeniem,
 - powiadomić w ciągu 72 godzin organ nadzoru w rozumieniu przepisów RODO o naruszeniu systemu informatycznego, jego przyczynach i skutkach oraz podjętych działaniach korygujących system, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,

§ 10

- Administrator prowadzi rejestr pracowników – użytkowników systemu informatycznego, zawierający:
- imię i nazwisko pracownika,
 - stanowisko,
 - zakres, w jakim pracownika dopuszczono do przetwarzania danych osobowych w systemie,

- datę wydania upoważnienia,
- datę utraty upoważnienia,
- indywidualny identyfikator pracownika.

§ 11

System informatyczny powinien zapewnić ujawnienie:

- daty wprowadzenia i modyfikacji danych osobowych,
- identyfikatora użytkownika systemu wprowadzającego dane,
- informację, komu, kiedy i w jakim zakresie dane zostały udostępnione,
- żądanie zaprzestania przetwarzania danych po jego uwzględnieniu.

§ 12

1. System informatyczny służący do przetwarzania danych osobowych musi pozwalać na udostępnienie tych danych na piśmie.
2. Dane przedstawione w formie pisemnej powinny zawierać informacje określone w § 11.

§ 13

1. Administrator określa pomieszczenia, w których przetwarzane są dane osobowe w systemie informatycznym.
2. Przebywanie osób nieuprawnionych oraz dostęp do danych osobowych w pomieszczeniach określonych w ust. 1 jest możliwe tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą Administratora.
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 osobom 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. Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, powinny być zabezpieczone przed utratą tych danych spowodowaną awarią i zakłóceniami sieci zasilającej.
6. Kopie zapasowe i archiwalne nie mogą być przechowywane w tych samych pomieszczeniach, w których są przetwarzane dane osobowe eksploatowane w bieżącej pracy.
7. Kopie zapasowe należy sprawdzić pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu i niezwłocznie usuwać te kopie po ustaniu ich przydatności.
8. 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 je w sposób uniemożliwiający ich odczytanie. W razie przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych - pozbawia się wcześniej zapisanych danych, a przy naprawie pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora.

III. POSTANOWIENIA SZCZEGÓLNE I KOŃCOWE

§ 14

1. Administrator może udostępnić dane osobowe członka Spółdzielni Walnemu Zgromadzeniu, Radzie Nadzorczej jedynie w przypadku, gdy w sprawie danego członka toczy się postępowanie wewnątrzspółdzielcze w trybie określonym w Statucie 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. Administrator 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 podmiotom uprawnionym do ich otrzymania na mocy przepisów ustawowych może nastąpić za zgodą Administratora na pisemnie umotywowany wniosek, chyba że przepis szczególny stanowi inaczej.
5. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
6. Odmowa udostępnienia danych osobowych następuje w przypadkach określonych przepisami RODO i ustawami .
7. Dane osobowe powinny być przechowywane przez okres, nie dłuższy niż niezbędny do celów, w których są przetwarzane tj.:
 - 1) w celu wypełnienia obowiązków prawnych nałożonych na podstawie ustawy z dnia 16 września 1982 r. Prawo spółdzielcze i ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (§ 4 ust. 1 pkt 1-3,5,8) -10 lat,
 - 2) po wyrażeniu zgody przez osobę, której dane dotyczą w jednym lub większej liczbie celów (§ 4 ust.1 pkt 4,6 i 7) – 10 lat,
 - 3) w celu wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (§ 4 ust. 1 pkt 4, 8) – osoby fizyczne przedsiębiorcy - 3 lata, osoby fizyczne nieprowadzące działalności gospodarczej -10 lat ,
 - 4) w celach wynikających z prawnie uzasadnionych interesów Spółdzielni lub osoby trzeciej (§ 4 ust. 1 pkt 3, 8 i 9) - 10 lat.
- 5) w celach związanych ze stosunkiem pracy, świadczeniami z ubezpieczeń społecznych i zdrowotnych pracowników zawarte w aktach osobowych i innych dokumentach w zakresie określonym przepisami Kodeksu pracy i stosownych ustaw – 50 lat od zakończenia pracy.

8. Umieszczanie nazwiska na spisie mieszkańców domu lub instalacji domofonowej jest możliwe po wyrażeniu pisemnej zgody przez osobę, której dane dotyczą.

9. Wzory dokumentów stosowanych w Spółdzielni w zakresie ochrony danych osobowych określa załącznik do niniejszej Instrukcji.