

Uchwała nr 21/2019

Rady Nadzorczej Spółdzielni Mieszkaniowej w Nowej Rudzie z dnia 30 sierpnia 2019 roku,

w sprawie: Regulaminu ochrony danych osobowych w Spółdzielni Mieszkaniowej w Nowej Rudzie.

Na podstawie Na podstawie § 54 ust. 1 pkt 8 lit. j Statutu Spółdzielni Mieszkaniowej w Nowej Rudzie uchwalonego przez Walne Zgromadzenie uchwałą nr 12/2018 z dnia 08-09 czerwca 2018 roku oraz art. 24 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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 (Dz. Urz. UE L 119/1 z 4.5.2016 r.) Rada Nadzorcza Spółdzielni Mieszkaniowej w Nowej Rudzie uchwała co następuje:

§ 1

Uchwała się regulamin ochrony danych osobowych w Spółdzielni Mieszkaniowej w Nowej Rudzie.

§ 2

Wykonanie uchwały powierza się Zarządowi Spółdzielni.

§ 3

Traci moc Uchwała Nr 04/2017 Rady Nadzorczej z dnia 24 lutego 2017 roku w sprawie regulaminu ochrony danych osobowych i informacji stanowiących tajemnice prawnie chronione w Spółdzielni Mieszkaniowej w Nowej Rudzie.

§ 4

Uchwała wchodzi w życie z dniem podjęcia.

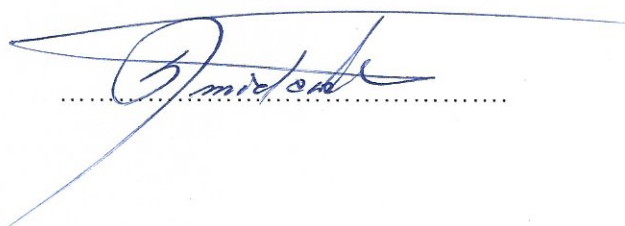
Głosowało⁸ członków Rady Nadzorczej:

...⁸ głosów "za",

.....⁰ głosów "przeciw",

.....⁰ głosów "wstrzymujących się".

Sekretarz Rady Nadzorczej
Jan Śmielewski



Przewodniczący Rady Nadzorczej
Andrzej Czernałowicz



REGULAMIN

ochrony danych osobowych w Spółdzielni Mieszkaniowej w Nowej Rudzie.

I. POSTANOWIENIA OGÓLNE.

§ 1

1. Niniejsza regulamin ochrony danych osobowych jest dokumentem opisującym sposób przetwarzania danych osobowych oraz obowiązki Spółdzielni Mieszkaniowej w Nowej Rudzie działającego w charakterze administratora danych osobowych, przetwarzanych w związku z prowadzoną działalnością.
2. Ilekroć w niniejszym regulaminie jest mowa o:
 - 1) Spółdzielni – należy przez to rozumieć Spółdzielnię Mieszkaniową w Nowej Rudzie,
 - 2) administratorze - należy przez to rozumieć Spółdzielnię,
 - 3) danych osobowych (dane) - należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
 - 4) naruszeniu ochrony danych osobowych - należy przez to rozumieć 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,
 - 5) odbiorcy - należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; nie są odbiorcami organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego,
 - 6) przetwarzanie - należy przez to rozumieć operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
 - 7) Rozporządzenie (RODO) - należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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,
 - 8) UODO (Urząd Ochrony Danych Osobowych) - należy przez to rozumieć organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych zbiorów 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.

§ 2

Administrator przetwarza dane osobowe z poszanowaniem poniższych zasad:

- 1) legalności - posiada odpowiednią podstawę prawną przetwarzania danych i na niej opiera to przetwarzanie;
- 2) rzetelności i prawidłowości - dba o aktualność danych oraz ich poprawność;
- 3) przejrzystości - przetwarza dane w sposób przejrzysty dla osoby, której dane dotyczą (w szczególności poprzez informowanie o przetwarzaniu danych);
- 4) celowości - przetwarza dane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza danych w sposób niezgodny z tymi celami;
- 5) adekwatności - dane są stosowne do celu, w jakim zostały zebrane;
- 6) minimalizacji - dane są przetwarzane w zakresie niezbędnym do celu, w jakim zostały pozyskane;
- 7) ograniczenia przechowywania - dane przechowywane są przez okres nie dłuższy, niż jest to niezbędne do celów w jakim dane osobowe zostały pozyskane;
- 8) integralności i poufności - dba o bezpieczeństwo danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

§ 3

Podstawę prawną niniejszego regulaminu stanowią w szczególności przepisy:

- 1) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 z późn. zm.);
- 2) ustawa z dnia 26 czerwca 1974 r. kodeks pracy (Dz. U. z 2019 r. poz. 1040.) - w odniesieniu do pracowników Spółdzielni;
- 3) ustawa z dnia 16 września 1982 r. Prawo spółdzielcze (Dz. U. z 2018 r. poz. 1285 z późn. zm.);
- 4) ustawa z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz. U. z 2018 r. poz. 845 z późn. zm.).

II. OCHRONA DANYCH OSOBOWYCH I ICH PRZETWARZANIE W SYSTEMIE INFORMATYCZNYM.

§ 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 przetwarza dane osobowe swoich członków i mieszkańców dla realizacji celów statutowych w zakresie:
 - 1) prowadzenia rejestru członków,
 - 2) prowadzenia rejestru lokali, w tym dla lokali, dla których zostały założone księgi wieczyste z adnotacją o ustanowionych hipotekach,
 - 3) listy przydziałów mieszkań,

- 4) sporządzania list niezbędnych dla obliczania opłat za używanie lokali,
 - 5) gromadzenia i przetwarzania danych osobowych zawartych w indywidualnych aktach członków Spółdzielni.
2. Spółdzielnia jako administrator 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 Administratora.
2. Administrator prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych oraz wydanych upoważnień.
3. Ewidencja, o której mowa w ust. 2, powinna zawierać:
 - 1) imię i nazwisko pracownika,
 - 2) stanowisko,
 - 3) zakres, w jakim pracownik został dopuszczony do przetwarzania danych osobowych,
 - 4) datę wydania upoważnienia,
 - 5) 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. Administrator dopuszcza do przetwarzania danych osobowych jedynie osoby upoważnione przez administratora, które złożyły oświadczenie o zachowaniu danych oraz sposobu ich zabezpieczeń w poufności. Obowiązek złożenia oświadczenia nie dotyczy osób uprawnionych do dostępu do danych osobowych z mocy przepisów prawa.

§ 7

1. Dane osobowe członków Spółdzielni i jej pracowników są przechowywane w wydzielonym i zabezpieczonym pomieszczeniu, określonym zarządzeniem Zarządu Spółdzielni.
2. Do pomieszczenia, o którym mowa w ust. 1, mogą mieć dostęp jedynie pracownicy Spółdzielni posiadający upoważnienie Administratora.
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 Administrator.

§ 8

Administrator stosuje środki techniczne oraz organizacyjne w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celu przetwarzania, ryzyka naruszenia

praw lub wolności o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. W szczególności administrator stosuje w tym celu:

- 1) pseudonimizację oraz szyfrowanie danych;
- 2) środki zapewniające poufność, integralność, dostępność danych oraz odporność systemów i usług przetwarzania;
- 3) środki zapewniające szybkie przywrócenie dostępności danych osobowych i dostęp do nich w razie incydentu fizycznego lub technicznego.

§ 9

1. Administrator przetwarza dane osobowe z poszanowaniem praw osób, których dane dotyczą wynikających z Rozporządzenia (RODO).
2. Administrator prowadzi rejestr zgłoszonych żądań, przez osoby, których danych dotyczą.
3. Przed wykonaniem praw osoby, której dane dotyczą administrator dokonuje weryfikacji tożsamości osoby zgłaszającej żądanie, celem ustalenia czy żądanie pochodzi od osoby uprawnionej.
4. Administrator zapewnia odpowiednie zaplecze techniczne oraz kadrowe w celu terminowej oraz rzetelnej realizacji praw osoby, której dane dotyczą. Zgłoszone żądania realizowane są przez administratora niezwłocznie, nie później niż w terminie miesiąca od otrzymania żądania. W przypadku niemożności wykonania żądania w w/w terminie, z uwagi na skomplikowany charakter sprawy, administrator informuje o przyczynie wydłużenia tego terminu oraz przewidywanym terminie realizacji żądania.

§ 10

1. Przy obsłudze systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania danych, mogą być zatrudnieni wyłącznie pracownicy posiadający upoważnienia wydane przez Administratora.
2. Administrator zapewnia przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz podejmowanie odpowiednich działań w przypadkach wykrycia naruszeń w systemie zabezpieczeń.

§ 11

1. Pracownikowi Spółdzielni zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym 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 co 30 dni.
5. Hasło powinno zawierać minimum 6 znaków, w tym litery duże i małe 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.

§ 12

1. Pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie informatycznym obowiązany jest niezwłocznie powiadomić administratora, gdy:
 - 1) stwierdzi naruszenie bezpieczeństwa 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 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,

§ 13

Administrator prowadzi rejestr pracowników - użytkowników systemu informatycznego, zawierający:

- 1) imię i nazwisko pracownika,
- 2) stanowisko,
- 3) zakres, w jakim pracownik został dopuszczony do przetwarzania danych osobowych w systemie informatycznym,
- 4) datę wydania upoważnienia,
- 5) datę utraty upoważnienia,
- 6) indywidualny identyfikator pracownika.

§ 14

System informatyczny powinien zapewniać odnotowanie:

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

§ 15

1. Administrator dokonuje bieżącego przeglądu czynności przetwarzania, celem weryfikacji, czy przetwarzanie to odbywa się w sposób zgodny z dokonaną oceną skutków dla ochrony danych osobowych.

2. Administrator konsultuje się z Urzędem Ochrony Danych Osobowych, jeżeli dokonana ocena skutków dla ochrony danych będzie wskazywała na występowanie wysokiego ryzyka dla praw osób których dane są przetwarzane.
3. W przypadku naruszeń ochrony danych osobowych mogących skutkować naruszeniem praw osób których dane dotyczą, administrator dokonuje zgłoszenia takiego naruszenia Urzędowi Ochrony Danych Osobowych.

§ 16

1. Administrator 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 przez Administratora możliwe jedynie 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.

§ 17

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.

§ 18

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 § 16 ust. 1, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§ 19

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.).

§ 20

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:
 - 1) okresowo sprawdzić pod kątem ich dalszej przydatności do odtwarzania danych w przypadku

awarii systemu,

2) bezzwłocznie usunąć po ustaniu ich użyteczności.

§ 21

3. Administrator korzysta wyłącznie z usług takich dostawców usług, którzy zapewniają odpowiednie gwarancje bezpieczeństwa danych osobowych i zgodności przetwarzania danych z przepisami Rozporządzenia.
4. Administrator dokonuje weryfikacji podmiotu przetwarzającego przed dokonaniem wyboru takiego podmiotu, jak również dokonuje jego późniejszej, okresowej weryfikacji, zgodnie z przyjętą u administratora procedurą, weryfikacja jest dokumentowana.
5. Administrator zawiera z podmiotem przetwarzającym umowę powierzenia przetwarzania danych osobowych lub reguluje okoliczność powierzenia przetwarzania danych innym instrumentem prawnym, w której określone zostają obowiązki podmiotu przetwarzającego wynikające z faktu powierzenia.

III. UDOSTĘPNIANIE DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ W NOWEJ RUDZIE.

§ 22

1. Administrator udostępni dane osobowe członka Spółdzielni Walnemu Zgromadzeniu, 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. Administrator 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.
4. 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.
5. Dokumenty udostępnione organom samorządowym nie mogą być wynoszone poza siedzibę Spółdzielni w żadnej postaci tj. oryginałów, kserokopii czy odpisów.
6. 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.

§ 23

1. Udostępnienie danych osobowych przetwarzanych przez Spółdzielnię osobom fizycznym lub instytucjom publicznym może nastąpić w trybie ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych oraz w Rozporządzeniu (RODO).
2. Tryb określony w ust. 1, Administrator uruchamia na pisemnie umotywowany wniosek.

3. Spółdzielnia może odmówić udostępnienia danych osobowych swoich członków i pracowników w przypadkach określonych w Rozporządzeniu (RODO) i w ustawie o ochronie danych osobowych.

§ 24

1. Osoba, której dane przetwarzane są przez Spółdzielnię ma prawo do informacji o:
- 1) sposobie przetwarzania danych osobowych (ręczne przetwarzanie danych, metody informatyczne, w tym sieci komputerowe),
 - 2) treści danych,
 - 3) sposobie udostępnienia danych osobowych oraz odbiorcach lub kategorii odbiorców danych.
2. Informacji, o których mowa w ust. 1, Administrator jest zobowiązany udzielić w terminie 30 dni od daty otrzymania wniosku.

Sekretarz Rady Nadzorczej



.....

Jan Śmielewski

Przewodniczący Rady Nadzorczej



.....

Andrzej Czerniatowicz