

REGULAMIN OCHRONY DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ „SADYBA” W KATOWICACH.

I. PODSTAWA PRAWNA:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. 2002 r. nr 101, poz. 926 z późniejszymi zmianami), zwana dalej ustawą.
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Cz. U. z 2004 r., nr 100, poz. 1025).
3. 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 informacyjne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., nr 100, poz. 1024).
4. Ustawa z dnia 16.09.1982 r. Prawo spółdzielcze (tj. Dz. U. 2003 r., Nr 188, poz. 1848 ze zm.).
5. Ustawa z dnia 15.12.2000 r. o spółdzielniach mieszkaniowych (tj. Dz. U. 2003 r., nr 119, poz. 1116 ze zm.).
6. Kodeks cywilny z dnia 23 kwietnia 1964 r. (tj. Dz. U. 2014 r. poz. 121).
7. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.
8. Ustawa z dnia 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U.nr 47poz. 211 z p. zm.).
9. Ustawa z dnia 06.06.1997 r. kodeks karny.
10. Ustawa z dnia 26.06.1974 r. kodeks pracy (jednolity tekst Dz. U. nr 21 poz. 94 z 1998 r. z p. zm.).
11. Statut Spółdzielni Mieszkaniowej „Sadyba” w Katowicach.

II. POSTANOWIENIA OGÓLNE.

§ 1.

1. Każdy ma prawo do ochrony dotyczących go danych osobowych.
2. Ochrona danych osobowych w Spółdzielni Mieszkaniowej „Sadyba” w Katowicach ma na celu zapewnienie każdemu członkowi Spółdzielni, nie-członkowi, mieszkańcowi, jej pracownikom i współpracownikom ochronę ich praw i wolności, w tym prywatności. Ponadto Spółdzielnia stosuje zabezpieczenia przed nieuprawnionym ujawnieniem danych osobowych, które może spowodować szkodę dla prawnie chronionych interesów Spółdzielni oraz wyżej wymienionych osób.
3. Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich, a także w związku z realizacją celów statutowych Spółdzielni Mieszkaniowej „SADYBA”, w zakresie i trybie określonym ustawą, statutem Spółdzielni i niniejszym regulaminem.
4. Regulamin niniejszy określa:
 - a. zasady i tryb przetwarzania danych osobowych, które znajdują się w posiadaniu Spółdzielni,
 - b. sposób zabezpieczenia zbiorów tychże danych osobowych i uniemożliwienie dostępu do zbioru danych osobom nieuprawnionym, a także zabezpieczenie ich przed uszkodzeniem lub zniszczeniem,
 - c. a także określa obowiązki administratora danych osobowych,
 - d. oraz prawa osób, których dane Spółdzielnia przetwarza.

§ 2.

Przez użyte w treści regulaminu sformułowania należy rozumieć:

1. Spółdzielnia - Spółdzielnię Mieszkaniową „SADYBA” z siedzibą w Katowicach,
2. Za dane osobowe - uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; czyli stanowi je każda informacja dotycząca osoby fizycznej pozwalająca na określenie tożsamości tej osoby;
3. Zbiór danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie; w szczególności prowadzony: w kartotekach, skorowidzach, księgach, wykazach, rejestrach, systemach informatycznych, aktach osobowych itp.;
4. przetwarzaniu danych - rozumie się przez to jakiegokolwiek operacje wykonywane na danych

- osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
5. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
 6. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
 7. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
 8. administrator danych osobowych (ADO) - podmiot zajmujący się przetwarzaniem danych osobowych. Administratorem danych osobowych jest Spółdzielnia Mieszkaniowa, a w jej imieniu zadania te wykonuje zarząd spółdzielni;
 9. administrator bezpieczeństwa informacji (ABI) - osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, wyznaczona przez administratora danych osobowych,
 10. zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie, zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie;
 11. odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
 - a. osoby, której dane dotyczą,
 - b. osoby upoważnionej do przetwarzania danych,
 - c. organów państwowych lub organów samorządu terytorialnego, którym dane są **udostępniane w związku z prowadzonym postępowaniem.**
 12. Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

§ 3.

1. Spółdzielnia, jako administrator danych osobowych przetwarza dane osobowe osób, o których mowa w § 1 ust. 2, w celu realizacji zadań statutowych obejmujących:
 - 1) prowadzenia rejestru członków,
 - 2) prowadzenia rejestru lokali, dla których zostały założone księgi wieczyste z adnotacją o ustanowionych hipotekach,
 - 3) sporządzania i ogłaszania list przydziałów mieszkań,
 - 4) sporządzania list niezbędnych dla obliczania opłat za użytkowanie lokali,
 - 5) gromadzenia i przetwarzania danych osobowych zawartych w indywidualnych aktach członków spółdzielni,
 - 6) wywieszania list lokatorów i umieszczania nazwisk przy instalacji domofonowej,
 - 7) sporządzania list niezbędnych do funkcjonowania organów samorządowych Spółdzielni,
 - 8) sporządzania zestawień i analiz związanych z eksploatacją zasobów mieszkaniowych i lokali użytkowych,
 - 9) prowadzenia korespondencji z właścicielami, użytkownikami lokali mieszkalnych i użytkowych,
 - 10) prowadzonych postępowań windykacyjnych sądowych i egzekucyjnych.
2. Spółdzielnia, jako administrator danych osobowych gromadzi i przetwarza dane osobowe swoich pracowników w zakresie wynikającym z Kodeksu pracy, przepisów wydanych na jego podstawie oraz przepisów szczególnych, poprzez gromadzenie i przetwarzanie akt osobowych pracowników Spółdzielni.
3. Zabrania się gromadzenia i przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym.
4. Dane dotyczące wskazań orzeczeń o ukaraniu i mandatach karnych, a także inne orzeczenia wydane w postępowaniu administracyjnym lub sądowym mogą być przetwarzane w celu realizacji praw i

obowiązków spółdzielni wynikających z tych orzeczeń.

5. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane zapewnić aby dane osobowe były:
 - a. wykorzystane zgodnie z prawem,
 - b. zbierane dla celów określonych w § 3 ust. 1,
 - c. aktualne a ich treść zgodna ze stanem faktycznym,
 - d. wykorzystane nie dłużej, niż wymaga tego realizacja celu dla którego zostały zgromadzone.
6. Czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża lub narusza interes przedsiębiorcy.
7. Spółdzielnia zobowiązuje się nie ujawniać informacji będących w jej posiadaniu, a dotyczących jej kontrahentów, w szczególności: informacje o adresach prywatnych osób reprezentujących kontrahenta, stosowanych przez niego technologiach, jego sytuacji finansowej, osiągniętych obrotach przedsiębiorstwa, informacji o ofertach i kontrahentach handlowych itp.

§ 4.

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mogą mieć wyłącznie osoby, które uzyskały pisemne upoważnienie wydane przez Administratora Danych Osobowych (ADO), chyba że upoważnienie do przetwarzania danych wynika bezpośrednio z przepisów prawa.
2. Osoby upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.
3. Pracownik, uzyskał upoważnienie do dostępu do zbioru danych osobowych i ich przetwarzania, powinien być zapoznany z przepisami dotyczącymi ochrony danych osobowych.
4. Pracownik Spółdzielni, który ma 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.
5. Upoważnienia, o których mowa w ust. 1 oraz oświadczenia pracowników, o których mowa w ust. 4, jest dołączona do akt osobowych pracownika.
6. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:
 - 01) imię i nazwisko osoby upoważnionej; stanowisko,
 - 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
- 13) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
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.

§ 5.

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

III. OCHRONA DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM.

§ 6.

1. Przy obsłudze systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być zatrudnieni wyłącznie pracownicy posiadający upoważnienie Zarządu Spółdzielni.
2. Pracownicy ci 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.

§ 7.

1. Obsługę systemu informatycznego mogą sprawować jedynie pracownicy posiadający upoważnienie wydane przez zarząd spółdzielni.
2. Jednocześnie Zarząd spółdzielni wyznacza „administratora bezpieczeństwa informacji” (ABI) odpowiedzialnego za bezpieczeństwo danych osobowych gromadzonych i przetwarzanych w systemie informatycznym.
3. 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, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 8.

1. Pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych w systemie informatycznym Administrator Bezpieczeństwa Informacji, (ABI) 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 przydzielane pracownikowi podlega cyklicznej zmianie.
5. Pracownik zatrudniony przy przetwarzaniu danych osobowych powinien utrzymywać w tajemnicy przydzielone mu hasło, także po upływie jego ważności.
6. Bezpośredni dostęp do systemu informatycznego zawierającego dane osobowe może nastąpić wyłącznie po podaniu identyfikatora i hasła.
7. Identyfikator osoby, która utraciła uprawnienia dostępu do systemu informatycznego zawierającego dane osobowe należy natychmiast wyrejestrować z systemu informatycznego i unieważnić hasło.

§ 9.

1. Pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie informatycznym obowiązany jest niezwłocznie powiadomić Zarząd i Administratora Bezpieczeństwa Informacji, gdy:
 - a. stwierdzi naruszenie zabezpieczenia 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 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 polegających na zabezpieczeniu systemu przed ponownym jego naruszeniem,
 - e. powiadomić Zarząd Spółdzielni o przyczynach i skutkach naruszenia systemu oraz podjętych działaniach korygujących system.

§ 10.

1. 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

- d. datę wydania upoważnienia,
 - e. datę utraty upoważnienia,
 - f. indywidualny identyfikator pracownika.
2. 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. żądanie zaprzestania przetwarzania danych po jego uwzględnieniu.

§ 11.

1. Zarząd spółdzielni może powierzyć przetwarzanie swoich danych innemu podmiotowi, w drodze pisemnej.
2. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 12.

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

§ 13.

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej.

§ 14.

Administrator bezpieczeństwa informacji obowiązany jest zabezpieczyć nośnik informacji, wydruki, kopie zapasowe, tak aby uniemożliwić dostęp do nich osobom nieuprawnionym lub przed ich uszkodzeniem lub zniszczeniem, zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29.IV.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 100 poz. 1024).

§ 15.

Szczegółowe zasady ochrony danych w systemie informatycznym zawiera „Polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym Spółdzielni Mieszkaniowej „SADYBA” w Katowicach opracowana przez Zarząd Spółdzielni. Instrukcja ta zawiera:

- a. Procedury nadawania i zmiany uprawnień do przetwarzania danych,
- b. Zasady posługiwania się hasłami,
- c. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie,
- d. Procedury tworzenia kopii zapasowych,
- e. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków,
- f. Sposób zabezpieczenia systemu informatycznego przed wirusami i szkodliwym oprogramowaniem,
- g. Procedury wykonywania przeglądów i konserwacji systemu,
- h. Procedury połączenia do sieci Internet,
- i. Zastosowanie środków bezpieczeństwa.

§ 16.

1. Archiwizowane dane nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco.
2. Dane, o których mowa w ust. 1 należy:
 - a. okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku

- awarii systemu,
b. bezzwłocznie usuwać po ustaniu ich użyteczności.

§ 17.

1. Udostępnienie danych osobowych członka Spółdzielni Walnemu Zgromadzeniu lub Radzie Nadzorczej możliwe jest jedynie w celu wykonywania kompetencji tych organów określonych w przepisach szczególnych i w zakresie określonym w tych przepisach.
2. Zarząd Spółdzielni jest zobowiązany do poinformowania członków organów Spółdzielni rozpatrujących sprawę członka Spółdzielni w postępowaniu wewnątrzspółdzielczym lub żądającym dostępu do danych osobowych członka spółdzielni o przepisach dotyczących ochrony danych osobowych.

§ 18.

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

§ 19.

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 w sieci komputerowej),
 - b. treści danych,
 - c. sposobie udostępnienia danych osobowych oraz odbiorcach lub kategorii odbiorców danych,- żądania uzupełnienia, uaktualnienia i sprostowania danych osobowych.
2. Informacji, o których mowa w ust. 1 Zarząd Spółdzielni jest zobowiązany udzielić w terminie 30 dni od daty otrzymania wniosku.

IV. POSTANOWIENIA KOŃCOWE.

§ 20.

Regulamin ochrony danych osobowych podaje do wiadomości każdemu pracownikowi upoważnionemu do dostępu i przetwarzania danych osobowych kierownik komórki organizacyjnej oraz udziela przeszkolenia w zakresie ochrony danych.

§ 21.

Zapoznanie z treścią tego regulaminu pracownik potwierdza w złożonym na piśmie oświadczeniu.

§ 22.

1. Nadzór nad przestrzeganiem regulaminu sprawują: Zarząd Spółdzielni oraz Administrator Bezpieczeństwa Informacji.
2. Udostępnienie przez Spółdzielnię danych objętych ustawą z dnia 29.08.1997 r. o ochronie danych osobowych, danych i dokumentów stanowiących tajemnicę przedsiębiorstwa a także innych danych prawem chronionych wymaga upoważnienia przepisów odpowiednich ustaw.

§ 23.

Sprawy nieujęte w niniejszym regulaminie określają przepisy ustawy, przepisy wykonawcze i przepisy szczególne.

§ 24.

Niniejszy regulamin został uchwalony przez Zarząd Spółdzielni w dniu 25.10.2014 Uchwałą Nr 24/2014 i obowiązuje od dnia uchwalenia.