POLITYKA

OCHRONY DANYCH OSOBOWYCH

Spółdzielni Mieszkaniowej „Nad Odrą" we Wrocławiu

zatwierdzona Uchwałą Zarządu nr 16/2018 z dnia 11.05.2018 r.

I. WPROWADZENIE

Niniejsza Polityka Ochrony Danych Osobowych (w dalszej części jako „Polityka") została opracowana w celu dostosowania działalności Spółdzielni Mieszkaniowej „Nad Odrą" we Wrocławiu do wymogów wynikających z 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 (ogólne rozporządzenie o ochronie danych – dalej jako „RODO").

Przygotowanie niniejszej instrukcji zostało poprzedzona analizą stanu ochrony danych osobowych, której zasadniczym celem było rozpoznanie ryzyk dla praw i wolności osób fizycznych wynikających z przetwarzania danych osobowych w Spółdzielni, określenie obowiązków Spółdzielni w zakresie ustanowienia inspektora ochrony danych oraz prowadzenia rejestru czynności przetwarzania oraz zaprojektowanie środków ochrony organizacyjnej i technicznej danych adekwatnych do rozpoznanych ryzyk związanych z ich przetwarzaniem.

Dane osobowe nie przetwarzane w Spółdzielni na znaczną skalę. Zasoby mieszkaniowe Spółdzielni obejmują ok. 200 lokali mieszkalnych i użytkowych oraz wynajmowane miejsca postojowe w parkingu wielostanowiskowym. Spółdzielnia przetwarza przede wszystkim dane osobowe użytkowników lokali mieszkalnych (członków spółdzielni i ich domowników oraz właścicieli lokale nie będących członkami spółdzielni). Przetwarzanie danych innych kategorii osób ma charakter ograniczony i dotyczy relatywnie niewielkiej ilości osób.

Przetwarzania danych użytkowników lokali mieszkalnych obejmuje następujące kategorie danych: imię i nazwisko, numer PESEL, imiona rodziców, adres zamieszkania lub adres

korespondencyjny, informacje o podstawie nabycia praw do lokali, dane o członkostwie w Spółdzielni, dane o stanie rozrachunków z tytułu opłat związanych z utrzymaniem lokali. Przetwarzanie tych kategorii danych osobowych jest niezbędne dla realizacji statutowych zadań Spółdzielni, a zatem stanowi główny przedmiot jej działalności w rozumieniu RODO.

Dane osobowe użytkowników lokali obejmują dane o ich stanie majątkowym (prawo do lokalu), ilości domowników, stanie rozrachunków ze Spółdzielnią. Jakkolwiek dane te nie należą do szczególnych kategorii danych w rozumieniu RODO z całą pewnością ewentualne naruszenie bezpieczeństwa ich przetwarzania wiązać się może z naruszeniem praw i wolności w postaci prawa do prywatności. W odniesieniu do tych kategorii osób nie zachodzi natomiast istotne ryzyko naruszenia innych praw i wolności (np. kradzież tożsamości, wyrządzenie istotnej szkody majątkowej, dyskryminacja).

Dane osobowe użytkowników lokali, obejmujące dane o zajmowanym lokalu, jego powierzchni, zużyciu mediów oraz stanie rozrachunków ze Spółdzielnią z tytułu należnych opłat przetwarzane są na podstawie odrębnej umowy przez podmiot zewnętrzny dostarczający usługi przetwarzania danych w tzw. chmurze obliczeniowej z wykorzystaniem dedykowanego oprogramowania wspierającego zarządzenie zasobami mieszkaniowymi.

Spółdzielnia przetwarza nadto **dane osobowe swoich pracowników** (zatrudnionych w pracowniczych i niepracowniczych formach zatrudnienia) oraz kontrahentów spółdzielni (dostawców towarów i usług dla celów realizacji zadań statutowych).

Dane osobowe pracowników obejmują informacje o stanie zdrowia pracowników i ich najbliższych, a to w związku z wykonywaniem przez Spółdzielnię obowiązków wynikających z przepisów prawa pracy i o zabezpieczeniu społecznym. W Spółdzielni nie funkcjonuje system wizyjnego monitoringu miejsc pracy, ani też żaden inny system monitorowania aktywności pracowników. Dane osobowe pracowników obejmujące informacje o ich stanie zdrowia (stanie zdrowia i sytuacji życiowej ich bliskich), stanie rodzinnym, zarobkach i potrąceniach z wynagrodzenia przetwarzane są przez podmiot przetwarzający, któremu na podstawie odrębnej umowy powierzono prowadzenie ksiąg rachunkowych i dokumentacji kadrowo-płaconej, a dostęp do nich jest ograniczony do tego podmiotu oraz członków Zarządu Spółdzielni. Dane te chronione są przy zastosowaniu środków technicznych i organizacyjnych opisanych w niniejszej Polityce.

Dane osobowe **kontrahentów** (najemców lokali użytkowych, dostawców towarów i usług) przetwarzane są wyłącznie w związku z zawieraniem i wykonywaniem umów; obejmują przede wszystkim dane dostępne w publicznych rejestrach oraz numery rachunków bankowych oraz informacje o stanie rozrachunków ze Spółdzielnią.

Na osiedlu funkcjonuje system monitoringu wizyjnego obejmującego bramę wjazdową na osiedla oraz okolice lokalu, w którym mieści się biuro Zarządu Spółdzielni.

Mając powyższe na uwadze przyjęto, iż Spółdzielnia, jako administrator danych osobowych, **prowadzi rejestr czynności przetwarzania**, o jakim mowa w art. 30 RODO. Niniejsza Polityka nie przewiduje natomiast obligatoryjnego powołania inspektora ochrony danych osobowych. Główna działalność Spółdzielni nie polega bowiem na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania na dużą skalę osób, których dane dotyczą, ani też nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawuje Zarząd Spółdzielni. Jeśli w Spółdzielni nie wyznaczono inspektora ochrony danych Zarząd wyznacza czy to spośród swoich członków, czy też innych osób wchodzących w skład personelu Spółdzielni, osobę odpowiedzialną za kontakty z Urzędem Ochrony Danych Osobowych (lub innym właściwym na podstawie obowiązujących przepisów organem nadzorczym) oraz wykonywanie uprawnień przysługującym osobom, których dane dotyczą.

Istotne ryzyka związane z przetwarzaniem danych osobowych w Spółdzielni stanowi:

- utrata przetwarzanych danych w skutek zdarzeń losowych lub bezprawnych działań osób trzecich
- ujawnienie danych, także danych obejmujących wiele osób, podmiotom nieuprawnionym, skutkujące naruszeniem prawa do prywatności osób, których dane dotyczą.

Szczególnym celem opracowania niniejszej Polityki jest ochrona przed niepowołanym dostępem do:

- systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;

- informacji zgromadzonych, przetwarzanych w formie tradycyjnej.

Z zapisami Polityki Ochrony Danych obowiązkowo są zapoznawani wszyscy członkowie personelu Spółdzielni uprawnieni do przetwarzania danych osobowych w jakimkolwiek zakresie.

Do informacji przechowywanych w systemach informatycznych jak i dokumentów tradycyjnych mają dostęp jedynie upoważnieni pracownicy Spółdzielni oraz osoby mające imienne zarejestrowane upoważnienie. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy.

Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi i organizacyjnymi. Opracowane procedury określają obowiązki użytkownika zbiorów tradycyjnych oraz zasady korzystania z systemów informatycznych.

Podstawę prawną przetwarzania danych osobowych użytkowników lokali stanowi art. 6 ust. 1 lit. c RODO w powiązaniu z odpowiednimi przepisami ustaw z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (t.j. Dz. U. z 2013 r. poz. 1222 z późn. zm.) i ustawy z dnia 24 czerwca 1994 r. o własności lokali (t.j. Dz. U. z 2018 r. poz. 716).

Podstawę prawną przetwarzania danych osobowych kontrahentów Spółdzielnia stanowi art. 6 ust. 1 lit. b RODO.

Podstawę prawną przetwarzania danych osobowych pracowników Spółdzielni stanowi art. 6 ust. 1 lit. b RODO w powiązaniu z odpowiednimi przepisami prawa pracy lub prawa cywilnego.

Podstawę przetwarzania danych zawartych w zapisach rozmów telefonicznych stanowi zgoda rozmówców.

II. DEFINICJE

Ilekroć w niniejszej Polityce mowa jest o:

a) **Administrator Systemu Informatycznego** – członek personelu Spółdzielni lub dostawca usług informatycznych upoważniony i zobowiązany do sprawowania bieżącego nadzoru nad funkcjonowaniem systemu informatycznego Spółdzielni

b) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej

c) **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych

d) **personelu Spółdzielni -** osoby zatrudnione na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia), osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej wykonujące prace związane z przetwarzaniem danych osobowych

e) **użytkowniku lokalu** – każdą osobę fizyczną posiadającą spółdzielcze prawo do lokalu mieszkalnego w zasobach Spółdzielni oraz właściciela lub współwłaściciela lokalu mieszkalnego lub niemieszkalnego wchodzącego w skład zasobów mieszkaniowych Spółdzielni

f) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych

g) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych i technik związanych z mechanicznym przetwarzaniem informacji zawierających dane osobowe utrwalonych w postaci dokumentu, z wyłączeniem dokumentów elektronicznych

III. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH

Spółdzielnia prowadzi ewidencję osób upoważnionych do ich przetwarzania danych osobowych, która obejmuje w szczególności:

a) imię, nazwisko i stanowisko osoby upoważnionej,
b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, w tym dostępu do poszczególnych modułów programu (aplikacji).

Wzór upoważnienia do przetwarzania danych osobowych oraz wzór ewidencji osób upoważnionych do przetwarzania danych stanowią załączniki nr 1 i 2 do niniejszej Polityki.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia. Oświadczenie o zapewnieniu ochrony danych osobowych stanowi załącznik nr 3 do niniejszej Polityki.

IV. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

A. BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH W FORMIE TRADYCYJNEJ

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. W przypadku konieczności opuszczenia pomieszczenia, w którym znajdują się zbiory danych osobowych, pomieszczenie powinno zostać zamknięte na klucz.

Dostęp do pokoi i szaf jest kontrolowany poprzez odnotowane pobieranie i zdawanie kluczy.

B. BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

Należy mieć świadomość, że każdy, kto ma dostęp do pomieszczenia, w którym zainstalowano sprzęt systemu informatycznego, może spowodować jego uszkodzenie lub może mieć dostęp do informacji wyświetlanych na monitorze lub wydruków. Zagrożenia w stosunku do systemu mogą pochodzić również od każdej innej osoby np. personelu pomocniczego, technicznego, konsultanta itp., posiadającej wystarczające umiejętności i wiedzę, aby uzyskać dostęp do sieci.

Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

Za nadawanie indywidualnych nazw użytkowników (tzw. loginów) oraz tymczasowych haseł do systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego.

Osoba nadająca uprawnienie, po nadaniu dostępu, przekazuje w sposób poufny hasło do systemu informatycznego użytkownikowi.

Nadanie uprawnienia do przetwarzania danych osobowych następuje na piśmie, wraz z pisemnym zobowiązaniem członka personelu do zachowania poufności danych osobowych oraz przestrzegania procedur ich przetwarzania.

Każdy użytkownik systemu informatycznego zobowiązany jest zapamiętać swoją nazwę użytkownika oraz hasło i nie udostępniać go innym osobom. Hasło tymczasowe podlega

zmianie przez użytkownika podczas pierwszego logowania się do systemu. Użytkownik systemu informatycznego powinien pamiętać o wylogowaniu się po zakończeniu korzystania z usług systemów informatycznych.

Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł o długości min. 8 znaków, nie trywialnych, tzn. nie może używać imion, danych identyfikujących użytkownika oraz jego najbliższych, oraz nie może tworzyć haseł przez kombinację tych nazw lub ich zmianę uporządkowania np. od tyłu. Hasło powinno składać się z liter, w tym przynajmniej jednej wielkiej litery oraz przynajmniej jednej cyfry lub znaku specjalnego. Zabrania się zapisywanie haseł przez użytkowników. W przypadku, gdy użytkownik zapomni swoje hasło, może on uzyskać nowe hasło od Administratora Systemu Informatycznego.

Do przetwarzania zbiorów danych osobowych w systemie informatycznym Spółdzielni, stosowane są pakiety biurowe przeznaczone do edycji dokumentów, oprogramowanie do obsługi kont poczty elektronicznej oraz aplikacje (programy) przeznaczone do zarządzania zasobami mieszkaniowymi i obsługi księgowej i kadrowo-płacowej.

KOMUNIKACJA W SIECI KOMPUTEROWEJ

Obieg dokumentów zawierających dane osobowe, pomiędzy poszczególnymi pracownikami Spółdzielni powinien odbywać się z wykorzystaniem **sieci lokalnej**, w sposób zapewniający ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

Przekazywanie informacji (danych) w systemie informatycznym **poza sieć lokalną** Spółdzielni odbywa się w relacji:

Spółdzielnia $\Rightarrow$ użytkownicy lokali – z wykorzystaniem poczty elektronicznej (e-mail) oraz aplikacji Weles3

Spółdzielnia $\Rightarrow$ kontrahenci – z wykorzystaniem poczty elektronicznej (e-mail)

Spółdzielnia $\Rightarrow$ Zakład Ubezpieczeń Społecznych – z wykorzystaniem programu Płatnik

Spółdzielnia $\Rightarrow$ Urząd Skarbowy – z wykorzystaniem dedykowanej platformy lub aplikacji księgowo płacowej

Spółdzielnia $\Rightarrow$ Banki – z wykorzystaniem systemu obsługi elektronicznej rachunku bankowego.

Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną Spółdzielni z wykorzystaniem poczty elektronicznej, powinno odbywać się w sposób **szyfrowany** (szyfrowane połączenie z serwerem pocztowym poczty przychodzącej i wychodzącej).

W przypadku przekazywania z wykorzystaniem poczty elektronicznej (e-mail) znacznej ilości danych osobowych dotyczących różnych osób bądź w przypadku przesłania taką drogę kopii dokumentów w formie załączników zaleca się by cała wiadomość albo załączone do niej załączniki zostały zaszyfrowane i zabezpieczone hasłem dostępu. Hasło dostępu umożliwiające otwarcie załącznika powinno, w miarę możliwości, zostać przekazane odbiorcy odrębnym kanałem komunikacji (sms, wiadomość e-mail przesłana na inny potwierdzony uprzednio adres).

Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie Administrator Systemu Informatycznego oraz upoważnieni pracownicy zapewniający ich prawidłową eksploatację. Wszyscy pracownicy, będący użytkownikami systemu zobowiązani są do zachowania tych danych w tajemnicy.

ŚRODKI OCHRONY

W Spółdzielni stosuje się niżej wymienione środki ochrony danych przetwarzanych w systemie informatycznym:

Środki ochrony fizycznej:

- urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi; komputery przenośne poza godzinami pracy zamykane są dodatkowo w zamykanych szafkach;
- dostęp do pokoi jest kontrolowany za pomocą wydawania kluczy tylko osobom uprawnionym;
- nośniki z kopiami zapasowymi zawierające dane osobowe przechowywane są w jednym pomieszczeniu w zamykanej na zamek patentowy metalowej szafie;
- komputery przenośne przechowane są szafach wyposażonych w zamki patentowe;
- dostęp do pomieszczenia, w którym znajdują się urządzenia serwerowe ma tylko Zarząd Spółdzielni oraz Administrator Systemu Informatycznego.

Środki sprzętowe, informatyczne i telekomunikacyjne:

- urządzenia wchodzące w skład infrastruktury sieciowej, serwery oraz komputery stacjonarne, na których przetwarzane są dane osobowe podłączone są do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania;
- sieć lokalna podłączona jest do Internetu poprzez router spełniający jednocześnie funkcję sprzętowego, zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną;
- kopie zapasowe wykonywane są automatycznie raz dziennie i przekazywane bezpośrednio na serwer;
- niedopuszczalne jest samowolne przemieszczenie lub zmiana konfiguracji stacji roboczej bez zgody Administratora Systemu Informatycznego.

Środki ochrony w ramach oprogramowania urządzeń teletransmisji:

- na komputerach użytkowników systemu działa program antywirusowy;
- na komputerach użytkowników systemu działa programowy firewall;
- dostęp do serwera zawierającego dane osobowe zabezpieczony jest hasłem.

Środki ochrony w ramach oprogramowania systemu:

- dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników;
- konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem dedykowanej aplikacji;
- zastosowano działający w tle program antywirusowy na komputerach użytkowników.

Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

- zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji;
- dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator;
- użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których przetwarzania są uprawnieni.

Środki ochrony w ramach systemu użytkowego (operacyjnego):

- komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym;
- stosuje się wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika;
- stosuje się blokadę hasłem podczas dłuższej nieaktywności użytkownika;
- nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego .

Środki organizacyjne:

- tymczasowe wydruki z danymi osobowymi są po ustaleniu ich przydatności niszczone;
- do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie indywidualnego pozwolenia na dostęp do przetwarzania danych osobowych wydawanego przez Zarząd Spółdzielni;
- osoby przetwarzające dane osobowe są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym;
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
- w przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą Spółdzielni, należy wymontować z niego nośniki informacji zawierające dane osobowe;
- w przypadku, gdy uszkodzenie sprzętu zawierającego nośnik danych, na którym zapisane są dane osobowe wymusza konieczność przekazania go poza siedzibę Spółdzielni, nośnik ten należy wymontować.

KONSERWACJE I NAPRAWY

Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje w szczególności jego aktualizację.

Przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza się czy spełnione są następujące wymagania:

- w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w szafie metalowej znajdującej się w strefie o ograniczonym dostępie (np. w szafie przeznaczonej do przechowywania kopii zapasowych danych);
- w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia;
- nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Systemu Informatycznego;
- zabrania się instalowania oprogramowania typu freeware czy shareware;
- należy regularnie uaktualniać bazę wirusów zainstalowanego oprogramowania antywirusowego;
- przed użyciem nośnika danych należy sprawdzić czy nie jest zainfekowany wirusem komputerowym.

KOPIE ZAPASOWE

Kopii należy dokonywać poprzez przegrywanie całej bazy danych (bez kompresji).

W każdej chwili powinna być dostępna kopia z poprzedniego tygodnia roku bieżącego (kopia tygodniowa) oraz kopia z roku ubiegłego (kopia roczna).

W czasie tworzenia kopii awaryjnej przez administratora, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany.

Nośniki elektroniczne przeznaczone do przechowywania danych osobowych powinny się charakteryzować odpowiednią trwałością zapisu, zależną od planowanego okresu przechowywania na nich danych.

Czas przechowywania kopii zapasowych zbiorów lokalnych ustala się na:

- kopia dzienna - 3 miesiące
- kopia roczna (ostatni dzień okresu bilansowego) - 5 lat

Wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane.

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas ewentualnego transportu i przechowywania tego

komputera, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych, w szczególności komputera nie należy pozostawiać w samochodzie.

V. UDOSTĘPNIANIE DANYCH OSOBOWYCH

ZASADY OGÓLNE

Do udostępniania przetwarzanych przez Spółdzielnię danych osobowych upoważniony jest pracownik Spółdzielni posiadający wymagane prawem upoważnienie.

Pracownik uprawniony do przetwarzania danych osobowych może dane te udostępnić wyłącznie innym członkom personelu Spółdzielni uprawnionym do przetwarzania danych osobowych oraz osobie, której dane dotyczą.

Przekazanie danych osobowych innym podmiotom możliwe jest wyłącznie w przypadkach wskazanych w niniejszej Polityce oraz gdy osoby te są do tego uprawnione na mocy przepisów prawa; w tym ostatnim przypadku wymaga zgody Zarządu Spółdzielni lub szczególnie umocowanego członka personelu (np. radcy prawnego lub inspektora ochrony danych, o ile zostanie on powołany).

UDOSTĘPNIENIA DANYCH OSOBOM, KTÓRYCH DANE DOTYCZĄ

Przekazywanie danych osobom, których dane dotyczą, następuje po **potwierdzeniu tożsamości** takiej osoby (odbiorcy danych). W przypadku udostępnienia danych w siedzibie Spółdzielni weryfikacja tożsamości odbiorcy danych polega na okazaniu dokumentu tożsamości (dowodu osobistego, paszportu, prawa jazdy).

W przypadku udostępnienia danych telefonicznie weryfikacja tożsamości odbiorcy danych polega na:

a) w przypadku udostępnienia **telefonicznego** informacji o stanie rozrachunków związanych z opłatami za lokale – na podaniu przez odbiorcę danych indywidulanego numeru ewidencyjnego przypisanego użytkownikowi lokalu

b) w innych przypadkach – możliwe jest wyłącznie po identyfikacji znanego członkowi personelu numeru telefonu rozmówcy – zaleca się by informacje obejmujące dane osobowe przekazywane były telefonicznie jedynie w niezbędnym zakresie; dane

dotyczące użytkowników lokali mogą być przekazywane tym osobom telefonicznie wyłącznie w zakresie dotyczącym bieżącego stanu rozrachunków z tytułu opłat oraz wysokości miesięcznych opłat związanych z użytkowanym przez te osoby lokalem.

W przypadku udostępnienia danych za pośrednictwem **poczty elektronicznej (e-mail)** weryfikacja tożsamości odbiorcy polega na:

a) w przypadku udostępnienia telefonicznego informacji o stanie rozrachunków związanych z opłatami za lokale – przesyłaniu korespondencji wyłącznie na adres poczty elektronicznej (e-mail) podany pisemnie przez osobę, której dane dotyczą

b) w pozostałych przypadkach - możliwe jest wyłącznie po identyfikacji znanego członkowi personelu adresu e-mail rozmówcy

W przypadku udostępnienia informacji o stanie rozrachunków związanych z opłatami za lokale **za pośrednictwem programu Weles3** użytkownicy lokali logują się do systemu za pomocą indywidualnych loginów i haseł. Użytkownik posiada dostęp wyłącznie do danych dotyczących jego lokalu oraz ogólnodostępnych danych dotyczących rozliczanej jednostki (budynku).

UDOSTĘPNIANIE DANYCH ODBIORCOM DANYCH

Dane osobowe przetwarzane w Spółdzielni mogą być przekazywane:

a) współpracującym ze Spółdzielnią kancelariom prawnym (adwokatom, radcom prawnym, spółkom radców prawnych i adwokatów) w celu dochodzenie roszczeń lub obrony przed roszczeniami;

b) zakładom ubezpieczeń lub brokerom ubezpieczeniowym w związku z toczącym się postępowaniem likwidacyjnym (w zakresie niezbędnym dla celów postępowania likwidacyjnego z wyłączeniem danych o stanie zobowiązań użytkowników lokali z tytułu opłat związanych z utrzymaniem i korzystaniem z lokali oraz czynszów najmu oraz spraw członkowskich);

c) dostawcom usług z zakresu utrzymania technicznego zasobów mieszkaniowych Spółdzielni – wyłącznie w zakresie danych kontaktowych użytkownika lokalu – na podstawie zgody osoby, której dotyczą lub po zawarciu z takim dostawcą pisemnej umowy o przetwarzanie danych osobowych;

d) członkom spółdzielni – w zakresie wynikającym z przepisu art. 8^1 ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (t.j. Dz. U. z 2018 r. poz. 845), tj. kopii uchwał organów spółdzielni i protokołów obrad organów spółdzielni, protokołów lustracji oraz faktur i umów zawieranych przez spółdzielnię z osobami trzecimi; tryb udostępniania tych dokumentów określa odrębny regulamin;

e) organom władzy publicznej na ich żądanie, o ile ma ono podstawę prawną;

f) innym podmiotom, o ile wykażą one interes prawny i podstawę prawną dla uzyskania dostępu do danych.

O udostępnieniu danych w przypadkach opisanych w pkt. e) i f) decyduje Zarząd Spółdzielni, po zasięgnięciu w razie potrzeby dodatkowej opinii działu prawnego Spółdzielni lub inspektora ochrony danych – o ile zostanie on ustanowiony.

Nie stanowi przekazania danych w rozumieniu niniejszej Polityki udostępnienie danych osobowych członka Spółdzielni Walnemu Zgromadzeniu lub Radzie Nadzorczej w przypadku, gdy w sprawie danego członka toczy się postępowanie wewnątrzspółdzielcze w trybie określonym postanowieniami statutu Spółdzielni. Dane osobowe członka Spółdzielni mogą być udostępnione organom Spółdzielni rozpatrującym jego sprawę w postępowaniu wewnątrzspółdzielczym tylko w zakresie mogącym mieć znaczenie dla sprawy.

Zarząd Spółdzielni jest zobowiązany do poinformowania członków innych organów Spółdzielni rozpatrujących sprawę członka Spółdzielni w postępowaniu wewnątrzspółdzielczym o zasadach dotyczących ochrony danych osobowych oraz uzyskać od tych osób pisemne oświadczenia o zobowiązaniu do zachowania poufności tych danych i przestrzegania zasad ich przetwarzania.

VI. UPRAWNIENIE OSÓB, KTÓRYCH DOTYCZĄ PRZETWARZANE DANE

OBOWIĄZKI INFORMACYJNE SPÓŁDZIELNI

Podczas pozyskiwania danych, a w przypadku pozyskania ich z innych źródeł niż osoba, której dotyczą, niezwłocznie po ich uzyskaniu, Spółdzielnia podaje osobom, których dane dotyczą, następujące informacje:

a) pełną nazwę Spółdzielni i dane kontaktowe;

b) informacje o źródle pochodzenia danych, jeśli nie pochodzą one od osoby, której dotyczą;

c) dane kontaktowe inspektora ochrony danych – o ile zostanie on ustanowiony;
d) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
f) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
g) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
h) jeżeli przetwarzanie odbywa się na podstawie zgody informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
i) informacje o prawie wniesienia skargi do organu nadzorczego;
j) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
k) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Obowiązki informacyjne Spółdzielni realizowane są co najmniej w następujących formach:

a) w odniesieniu do użytkowników lokali – w postaci broszur informacyjnych dostarczanych bezpośrednio użytkownikom lokali i dostępnych w siedzibie Spółdzielni; broszury informacyjne mogą być dostarczane osobom, których dane są już przetwarzane w chwili wejścia w życie niniejszej Polityki oraz osobom, których dane pozyskano z innych źródeł niż te osoby wraz z inną korespondencją w terminach wynikających potrzeb organizacyjnych Spółdzielni;
b) w odniesieniu do pracowników – na piśmie, przy nawiązaniu stosunku pracy;
c) w stosunku do kandydatów do zatrudnienia – poprzez zamieszczenie w ogłoszeniach o rekrutacji informacji o możliwości zapoznania się z informacjami na stronie internetowej spółdzielni lub w jej siedzibie;
d) w stosunku do najemców lokali użytkowych – na piśmie, przy zawarciu umowy;

e) w stosunku do dostawców usług i towarów - poprzez zamieszczenie w umowach, zamówieniach lub ofertach informacji o możliwości zapoznania się z informacjami na stronie internetowej spółdzielni lub w jej siedzibie;
f) w stosunku do interesantów (nagrania rozmów telefonicznych) – poprzez informacje udzielane przez automat podczas realizacji połączenia z odesłaniem do informacji opublikowanych na stronie internetowej Spółdzielni;
g) w stosunku do wszystkich kategorii osób – poprzez publikacje stosownych informacji na stronie internetowej spółdzielni.

SZCZEGÓLNE UPRAWNIENIA ZWIĄZANE Z PRZETWARZANIEM DANYCH

Osobom, których dotyczą przetwarzane przez Spółdzielnię dane osobowe przysługują w szczególności następujące uprawnienia:

- wglądu do swoich osobowych oraz prawo do domagania się sprostowania lub aktualizacji danych nieścisłych,
- usunięcia danych, chyba że nie upłynął jeszcze okres ich zamierzonego przetwarzania a dalsze ich przetwarzanie nie jest uzasadnione potrzebą ustalenia, dochodzenia lub obrony roszczeń,
- żądania ograniczenia przetwarzania danych osobowych - po zgłoszeniu takiego żądania dane te nie będą przetwarzane z wyjątkiem ich przechowywania; mogą jednak w dalszym ciągu być przetwarzane w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej,
- uzyskania kopi danych podlegających przetwarzaniu.

Wszelkie **wnioski i oświadczenia związane z przetwarzaniem danych osobowych, osoby, których dane te dotyczą, mogą zgłaszać pisemnie lub za pośrednictwem poczty elektronicznej.** Oświadczenia, wnioski i żądania dotyczące przetwarzania danych osobowych mogą być składana w formie elektronicznej, **wyłącznie z wykorzystaniem wskazanego uprzednio na piśmie adresu poczty elektronicznej**. Tylko ten adres poczty elektronicznej będzie mógł być wykorzystywany do celów komunikacji związanej z przetwarzaniem danych osobowych.

W przypadku zgłoszenia żądania poprawienia danych nieścisłych, ich aktualizacji lub uzupełnienia, a także w przypadku zgłoszenia żądania ograniczenia przetwarzania danych lub ich usunięcia Spółdzielnia informuje osobę zainteresowaną o sposobie załatwienia wniosku lub żądania najdalej **w terminie 30 dni** od jego zgłoszenia. W uzasadnionych przypadkach termin ten może zostać przedłużony o dalsze 2 miesiące.

Z uwagi na fakt, iż podstawą przetwarzania danych użytkowników lokali nie jest ani zgoda, ani umowa zawarta ze Spółdzielnią osobom tym nie przysługuje uprawnienia do domagania się przeniesienia danych, o jakim mowa w art. 20 RODO. Dane osobowe innych kategorii osób (pracowników, najemców) mogą podlegać prawu ich przenoszenia w zakresie, w jaki będą one przetwarzane w sposób zautomatyzowany.

VII. PRZETWARZANIE DANYCH OSOBOWYCH W ZATRUDNIENIU

Przetwarzanie danych osobowych w zatrudnieniu dopuszczalne jest wyłącznie w zakresie niezbędnym dla nawiązania i realizacji stosunku pracy. Postanowienie niniejszej Polityki nie uchybiają szczególnym przepisom prawa pracy i prawa ubezpieczeń społecznych, w zakresie w jakim określają one dopuszczany zakres i tryb przetwarzania danych osób zatrudnionych.

Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Spółdzielnia może żądać udokumentowania danych osobowych pracownika lub kandydata na pracownika, jeżeli uzna za konieczne ich potwierdzenie.

PRZETWARZANIE DANYCH W PROCESIE REKRUTACJI

Od osoby ubiegającej się o zatrudnienie Spółdzielnia może zażądać podania danych osobowych obejmujących:

a) imię (imiona) i nazwisko;
b) datę urodzenia;
c) adres do korespondencji;
d) adres poczty elektronicznej albo numer telefonu;
e) wykształcenie;
f) przebieg dotychczasowego zatrudnienia.

Spółdzielnia może żądać podania innych danych osobowych, w tym w szczególności informacji (np. danych o karalności) jeżeli obowiązek ich podania wynika z odrębnych

przepisów lub gdy jest to niezbędne do wypełniania obowiązku pracodawcy nałożonego przepisem prawa.

Dane te przetwarzane są wyłącznie w celu rekrutacji, w wyodrębnionym w tym celu zbiorze i usuwane niezwłocznie po zakończeniu procesu rekrutacji, chyba że ich dalsze przetwarzanie uzasadnione jest zatrudnieniem osoby, której dane dotyczą.

PRZETWARZANIE DANYCH PRACOWNIKÓW

Spółdzielnia może żądać od pracownika podania danych osobowych obejmujących:

a) adres zamieszkania;
b) numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość;
c) inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy.

Spółdzielnia może żądać podania innych danych osobowych (np. danych o karalności) jeżeli obowiązek ich podania wynika z odrębnych przepisów lub gdy jest to niezbędne do wypełniania obowiązku pracodawcy nałożonego przepisem prawa.

Spółdzielnia przechowuje orzeczenia wydane na podstawie wstępnych, kontrolnych i okresowych badań lekarskich oraz, w odpowiednich przypadkach, skierowania na wykonanie takich badań wystawione przez innych pracodawców pracownika.

W przypadku stwierdzenia, że warunki określone w skierowaniu na badania wstępne, okresowe lub kontrolne wystawionemu przez innego pracodawcę nie odpowiadają warunkom występującym na danym stanowisku pracy, Spółdzielnia zwraca osobie przyjmowanej do pracy to skierowanie oraz orzeczenie lekarskie wydane w wyniku tego skierowania.

VIII. MONITORING WIZYJNY

Z uwagi na konieczność zapewnienia bezpieczeństwa osób i mienia okolica bramy wjazdowej na osiedle oraz okolica lokalu, w którym znajduje się biuro Zarządu Spółdzielni objęte są systemem monitoringu wizyjnego.

Nagrania obrazu przetwarza się wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres 2 tygodni od dnia nagrania (automatyczne nadpisywanie danych).

W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub w przypadku powzięcia wiadomość, iż mogą one stanowić dowód w postępowaniu, termin określony powyżej ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

Po upływie okresów przetwarzania opisanych powyżej uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe, podlegają zniszczeniu.

Użytkownicy lokali są informowani o wprowadzeniu monitoringu i celach przetwarzania danych w ten sposób pozyskanych w tym samym trybie w jaki informuje się ich o przetwarzaniu innych kategorii danyc. Teren monitorowany oznacza się w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych.

IX. PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

ZASADY OGÓLNE

Naruszenie ochrony danych to naruszenie bezpieczeństwa ich przetwarzania 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.**

Każdy członek personelu Spółdzielni, który stwierdzi fakt naruszenia ochrony danych osobowych w Spółdzielni, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo przetwarzania danych osobowych jest zobowiązany poinformować Zarząd Spółdzielni o tego rodzaju zdarzeniach. Naruszenie ochrony danych osobowych lub zagrożenie bezpieczeństwa przetwarzania danych w systemie informatycznym powinno zostać głoszone także Administratorowi Systemu Informatycznego.

Niezwłocznie po dowiedzeniu się o naruszeniu ochrony danych osobowych Zarząd Spółdzielni:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie dla bezpieczeństwa przetwarzania danych osobowych oraz konieczności zabezpieczenia bieżącej działalności Spółdzielni;
- żąda dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
- dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport obejący w szczególności okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Zagrożenie bezpieczeństwa przetwarzania danych, nieskutkujące naruszeniem ochrony danych osobowych, może stać się przedmiotem analizy przeprowadzanej przez Zarząd. Analiza ta powinna zawierać wszechstronną ocenę zaistniałego zdarzenia, ewentualne wskazanie osób odpowiedzialnych oraz wnioski co do ewentualnych działań proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

ZAWIADOMIENIE OGRANU NADZORCZEGO O NARUSZENIU OCHRONY DANYCH

W terminie 72 godzin od powzięcia informacji o zaistniałym **naruszeniu ochrony danych** tj. przypadkowym lub niezgodnym z prawem zniszczeniu, utracenie, zmodyfikowaniu, nieuprawnionym ujawnieniu lub nieuprawnionym dostępie do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Spółdzielnią, Zarząd Spółdzielni zgłasza takie zdarzenie Prezesowi Urzędu Ochrony Danych Osobowych (lub innemu właściwemu na podstawie obowiązujących przepisów organowi nadzorczemu).

W zakresie, w jakim informacji wymaganych w zgłoszeniu nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

Zgłoszenie naruszenia ochrony danych:

a) opisuje charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawiera imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisuje możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisuje środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH

Jeżeli naruszenie ochrony danych osobowych może powodować **wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, administrator bez zbędnej zwłoki zawiadamia się osobę, której dane dotyczą, o takim naruszeniu.

Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera:

a) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
b) opisuje możliwe konsekwencje naruszenia ochrony danych osobowych;
c) opisuje środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie nie jest wymagane, w następujących przypadkach:

a) administrator wdrożył w odniesieniu do danych osobowych, których dotyczy naruszenie środki ochrony (np. szyfrowanie) uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
c) wymagałoby ono niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

X. POSTANOWIENIE KOŃCOWE

Niniejsza polityka wchodzi w życie z dniem 25 maja 2018 r.

W okresie 24 miesięcy od dnia wejścia w życie niniejszej Polityki, a następnie, nie rzadziej niż co 36 miesięcy Spółdzielnia dokona przeglądu funkcjonowania przetwarzania danych osobowych w kontekście przestrzegania zasad wynikających z niniejszej Polityki oraz zmian w zakresie przetwarzania danych osobowych wynikających z postępu technologicznego, ewentualnych zmian organizacyjnych w działalności Spółdzielni oraz ujawniających się zagrożeń dla praw i wolności osób związanych z przetwarzaniem danych osobowych.

Integralną część niniejszej Polityki stanowią załączniki w postaci:

1) wzoru upoważnienie do przetwarzania danych osobowych,
2) wzoru ewidencji osób upoważnionych do przetwarzania danych osobowych,
3) wzoru oświadczenie o zapoznaniu się z zasadami dotyczącymi ochrony danych osobowych i zobowiązania do zachowania ich poufności,
4) wzoru oświadczenia członka Rady Nadzorczej o zapoznaniu się z zasadami dotyczącymi ochrony danych osobowych i zobowiązania do zachowania ich poufności,
5) rejestru czynności przetwarzania.

Wrocław, dnia ... r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym upoważniam:

……

(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w:

Spółdzielni Mieszkaniowej „Nad Odrą” z/s we Wrocławiu

na stanowisku:

do przetwarzania od dnia danych osobowych

w zakresie

……

……

……

Upoważnienie wygasa z chwilą rozwiązania umowy o pracę/umowy zlecenia lub w związku ze zmianą stanowiska pracy.

Wnoszę/nie wnoszę* o nadanie identyfikatora użytkownika i przyznanie hasła do obsługi systemu informatycznego.

EWIDENCJA OSÓB UPRAWNIONYCH DO PRZETWARZANIA DANYCH								
LICZBA PORZĄDKOWA UPOWAŻNIENIA	**DANE PERSONALNE PRACOWNIKA (IMIĘ I NAZWISKO)**	**OZNACZENIE KOMÓRKI ORGANIZACYJNEJ**	**NAZWĘ UŻYTKOWANEGO PROGRAMU (APLIKACJI),**	**ZAKRES DOSTĘPU DO UŻYTKOWANEGO PROGRAMU (APLIKACJI)**	**OKREŚLENIE KATEGORII DANYCH DO KTÓRYCH PRZETWARZANIA UPOWAŻNIONY JEST PRACOWNIK**	**DATĘ WPROWADZENIA DO REJESTRU,**	**DATĘ USUNIĘCIA Z REJESTRU,**	**WAŻNOŚĆ UPOWAŻNIENIA**

OŚWIADCZENIE

O ZOBOWIĄZANIU DO PRZESTRZEGANIA ZASAD OCHRONY DANYCH OSOBOWYCH

Zobowiązuję się do przestrzegania obowiązujących w Spółdzielni Mieszkaniowej „Nad Odrą" we Wrocławiu zasad ochrony danych osobowych oraz obowiązujących w tym zakresie przepisów prawa powszechnie obowiązującego.

Potwierdzam, iż zostałem (am) zapoznany (a) z obowiązującą Polityką Ochrony Danych Osobowych.

Zobowiązuje się do zachowania poufności przetwarzanych danych w okresie zatrudnienia jak i po ustaniu zatrudnienia.

……

/ imię i nazwisko, data/

OŚWIADCZENIE

członka Rady Nadzorczej SM „Nad Odrą” we Wrocławiu

mającego dostęp do danych osobowych

Ja niżej podpisany (a) ,

członek Rady Nadzorczej SM „Nad Odrą” we Wrocławiu oświadczam, że zapoznałem(am) się z treścią Polityki Bezpieczeństwa i Regulaminu Ochrony Danych Osobowych w Spółdzielni i zobowiązuję się do ich przestrzegania oraz zachowania w tajemnicy powierzonych mi danych osobowych, również po zakończeniu działalności w Radzie Nadzorczej.

……

/ imię i nazwisko, data/