Załącznik nr 1
do Uchwały Rady Nadzorczej nr
04/2022
Spółdzielnia Mieszkaniowa
Pracowników Wsk Pzl Kraków
z dnia 12.09.2022 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH
Spółdzielnia Mieszkaniowa Pracowników Wsk Pzl Kraków

Polityka ochrony danych osobowych Spółdzielni Mieszkaniowej Pracowników Wsk Pzl Kraków, określa zasady postępowania, stosowane środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa w zakresie ochrony danych osobowych przetwarzanych w formie papierowej oraz w systemach informatycznych.
Aby przetwarzanie odbywało się w sposób zapewniający należytą ochronę danych osobowych będących w zasobach Administratora Danych Osobowych, przetwarzanie odbywa się z zachowaniem następujących zasad:

- zgodności z prawem;
- rzetelności, przejrzystości i ograniczoności celu;
- adekwatności, prawidłowości i okresowości przetwarzanych danych;
- poufności, integralności i rozliczalności danych.

Spółdzielnia Mieszkaniowa Pracowników Wsk Pzl Kraków dąży do systematycznego unowocześniania stosowanych w jego strukturze fizycznych, informatycznych oraz organizacyjnych środków ochrony danych osobowych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

I. SŁOWNIK POJĘĆ

Ilekroć w niniejszej Polityce Ochrony Danych Osobowych używane są poniższe pojęcia, mają one następujące znaczenie:

Administrator Danych Osobowych	oznacza Spółdzielnia Mieszkaniowa Pracowników Wsk Pzl Kraków z siedzibą przy ul. Wybickiego 3, 31-261 Kraków, reprezentowaną przez Zarząd.
Anonimizacja	oznacza proces prowadzący do nieodwracalnego uniemożliwienia zidentyfikowania osoby fizycznej. W celu zanonimizowania jakichkolwiek danych, dane te muszą zostać pozbawione wystarczającej liczby elementów, tak aby nie było już możliwości zidentyfikowania osoby, której dane dotyczą, tj. dane należy przetwarzać w taki sposób, aby nie istniała już możliwość wykorzystania ich do zidentyfikowania osoby fizycznej za pomocą wszelkich sposobów, jakimi może posłużyć się administrator danych lub osoba trzecia.
Dane osobowe	oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do identyfikowania osobie fizycznej, w

	szczególności: imię, nazwisko, adres, PESEL, numer telefonu, e-mail NIP, nr członkowski itp.
Dane osobowe szczególnych kategorii (dane wrażliwe)	oznaczają dane osobowe ujawniające pochodzenie etniczne lub rasowe, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące stanu zdrowia osoby fizycznej, jej seksualności lub orientacji seksualnej.
Kodeks pracy	oznacza ustawę z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 108 z późn. zm.)
Organ nadzorczy lub PUODO	oznacza Prezesa Urzędu Ochrony Danych Osobowych
Osoba współpracująca	oznacza osobę świadczącą usługi na rzecz Spółdzielni Mieszkaniowej Pracowników Wsk Pzl Kraków, na podstawie umowy cywilnoprawnej, umowy o współpracy, w ramach której przetwarzane są dane osobowe
Podmiot przetwarzający	oznacza organizację lub osobę, której Administrator Danych Osobowych powierzył przetwarzanie danych osobowych
Polityka	oznacza niniejszą Politykę Ochrony Danych Osobowych
Pracownik	oznacza osobę zatrudnioną w Spółdzielni Mieszkaniowej Pracowników Wsk Pzl Kraków na podstawie powołania, mianowania, umowy o pracę, spółdzielczej umowy o pracę, oraz powołania na zasadach innych niż Kodeks pracy
Pseudonimizacja	oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Pseudonimizacja ogranicza możliwość tworzenia powiązań zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą; technika ta stanowi użyteczny środek bezpieczeństwa, nie jest natomiast metodą anonimizacji.
Przetwarzanie danych osobowych	oznacza operację, lub zestaw operacji dokonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany (np. zbieranie, przeglądanie, rozpowszechnianie, modyfikowanie, niszczenie itd.).
RODO	oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z prze-

	twarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 2016-04-27 (Dz.Urz.UE.L 2016 Nr 119, str. 1)
Ustawa o ochronie danych osobowych	oznacza ustawę z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000)
System informatyczny	oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
Spółdzielnia Mieszkaniowa	oznacza Spółdzielnia Mieszkaniowa Pracowników Wsk Pzl Kraków. z siedzibą w Krakowie ul. Wybickiego 3, 31-261 Kraków
Użytkownik	oznacza każdą osobę posiadającą uprawnienia dostępu do systemu informatycznego Spółdzielni Mieszkaniowej

II. ZAKRES PODMIOTOWY

1. Postanowienia niniejszej Polityki mają zastosowanie do pracowników Spółdzielni Mieszkaniowej, jak również do wszystkich osób i podmiotów mających dostęp do danych osobowych w związku z wykonywaniem określonych zadań lub na podstawie umów o pracę, umów zawartych ze Spółdzielnią, w tym również osób współpracujących na zasadach B2B, umów zleceń, umów o dzieło oraz osób powołanych.
2. Celem wprowadzenia niniejszej Polityki jest:
    1) zagwarantowanie pełnej ochrony danych osobowych jak również zapewnienie ciągłości procesu ich przetwarzania,
    2) zapewnienie przestrzegania zasad przetwarzania danych osobowych, tj.: legalności, przejrzystości, rzetelności, celowości, adekwatności, prawidłowości, czasowości, integralności oraz poufności przetwarzania danych osobowych osób fizycznych,
    3) dążenie do ograniczania zagrożeń dla bezpieczeństwa danych osobowych.
3. Za dokonywanie przeglądów oraz aktualizację niniejszej Polityki odpowiada Administrator Danych Osobowych.

III. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

A. Zasada zgodności z prawem

1. Przetwarzanie danych osobowych winno być zgodne z prawem, rzetelnie i dokonywane w sposób przejrzysty dla osoby, której dane dotyczą.
2. Rzetelność oznacza uczciwe i lojalne przetwarzanie danych osobowych względem osób, których dane dotyczą.
3. Przejrzystość oznacza czytelną i zrozumiałą komunikację Administratora Danych Osobowych z osobą, której dane dotyczą. Oznacza to obowiązek jasnego i czytelnego formułowania np. klauzul informacyjnych oraz zgód na przetwarzanie danych osobowych.
4. Przetwarzanie danych osobowych uznaje się za zgodne z prawem, jeżeli:

a) osoba której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych w jednym lub większej ilości celów,
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
c) przetwarzanie danych jest niezbędne do wykonania obowiązku prawnego ciążącego na Administratorze Danych Osobowych,
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy powierzonej Administratorowi Danych Osobowych,
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych Osobowych lub przez osobę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem.

5. Przetwarzanie szczególnych kategorii danych osobowych uważa się za zgodne z prawem, wyłącznie w następujących przypadkach:
a) osoba, której dane dotyczą wyraziła wyraźną zgodę na przetwarzanie danych osobowych w jednym lub w kilku konkretnych celach,
b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora Danych Osobowych lub osobę, której dane dotyczą, w dziedzinie prawa pracy, o ile przepisy szczególne nie stanowią inaczej;
c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
d) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
e) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
f) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
g) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego;
h) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

i) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na podstawie obowiązujących przepisów.

6. W przypadkach opisanych w ust. 4 lit. a lub ust. 5 lit. a powyżej, Administrator Danych Osobowych winien dysponować zgodą osoby, której dane dotyczą wyrażoną w formie pisemnej lub elektronicznej.

B. Zasada celowości

1. Zasada celowości oznacza, iż dane osobowe winny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
2. Przetwarzanie danych osobowych winno następować wyłącznie dla zgodnych z prawem celów, jak również nie powinno być poddawane dalszemu przetwarzaniu dla innych celów, chyba że istnieje do tego podstawa prawna a osoba, której dane dotyczą została poinformowana o tym innym celu.
3. Niedopuszczalne jest zatajenie lub pominięcie któregokolwiek z celów, w jakim mają być przetwarzane dane osobowe.
4. Dalsze przetwarzanie danych osobowych lub szczególnych kategorii danych osobowych do celów archiwalnych w interesie publicznym, do celów np. statystycznych uznawane jest za operacje przetwarzania zgodne z prawem i z pierwotnymi celami, pod warunkiem przestrzegania zasady proporcjonalności.
5. Cel przetwarzania danych w Spółdzielni Mieszkaniowej stanowi w szczególności:
   a) realizacji procesu współpracy na zasadach B2B,
   b) prowadzenie polityki kadrowej i księgowej,
   c) w celu spełniania obowiązków i realizacji uprawnień wynikających ze stosunku członkostwa, z faktu posiadania tytułu prawnego do lokalu pozostającego w zasobach Spółdzielni lub użytkowania takiego lokalu,
   d) w celu spełniania obowiązków i realizacji uprawnień wynikających z faktu posiadania tytułu prawnego do lokalu pozostającego w zasobach Administratora lub użytkowania takiego lokalu,
   e) w celu wypełnienia ciążących na Administratorze obowiązkach prawnych, w szczególności z tytułu przepisów rachunkowo-podatkowych przez okres przewidziany w przepisach prawa,
   f) w celach wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora), co oznacza w szczególności obsługę, dochodzenie i obronę przed ewentualnymi roszczeniami przez okres przedawnienia roszczeń określony w przepisach prawa,
   g) w związku z przeprowadzeniem procesu przetargowego mającego wyłonić wykonawcę dane osobowe oferenta są przetwarzane w ramach czynności zmierzających do podpisania umowy przez okres: w przypadku ofert, które zostały wyłonione w drodze przetargu do momentu przedawnienia roszczeń z tytułu zawartej umowy. Natomiast dane zawarte w ofertach, które nie zostały wyłonione w drodze przetargu 3 lata.
   h) dane pracowników oferenta przetwarzamy w ramach realizacji prawnie uzasadnionego interesu Administratora w związku z potwierdzeniem kwalifikacji niezbędnych do wykonania zadania objętego postępowaniem przetargowym przez okres: w przypadku ofert, które zostały wyłonione w drodze przetargu do momentu przedawnienia roszczeń z tytułu zawartej umowy. Natomiast dane zawarte w ofertach, które nie zostały wyłonione w drodze przetargu 3 lata.

i) w celach związanych z uczestnictwem w przetargu ustnym nieograniczonym, realizowanym w formie licytacji lub pozyskiwania pisemnych ofert, którego celem jest ustanowienie odrębnej własności lokalu mieszkalnego oraz w związku z udokumentowaniem jego przebiegu przez okres 3 lat a także realizacją obowiązków prawnych zgodnie z przepisami rachunkowymi i podatkowymi.

j) w celu wykonania umowy np. najmu, dzierżawy, dotyczącej realizacji zamówienia przez okres jej trwania, a później przez wzgląd ma obowiązki rachunkowe przez okres przewidziany w przez okres przewidziany w odpowiednich przepisach prawa lub do momentu przedawnienia ewentualnych roszczeń.

k) celem wykonania niezbędnych napraw zgłaszanych przez mieszkańców, realizując prawnie uzasadniony interes Administratora przez okres 5 lat.

l) monitoring wizyjny realizowany jest jako prawnie uzasadniony interes Administratora w postaci zapewnienia bezpieczeństwa oraz gromadzenia materiału dowodowego ewentualnych naruszeń. Obszar monitorowany został oznaczony tablicami informacyjnymi oraz piktogramami kamer. Zapisy z monitoringu przechowywane będą nie dłużej niż 14 dni od daty nagrania. Okres ten może ulec wydłużeniu w przypadku, w którym nagranie stanowi dowód w postępowaniu prowadzonym na podstawie prawa lub Administrator powziął wiadomość, iż mogą one stanowić dowód w postępowaniu. Termin ten ulega przedłużeniu do czasu prawomocnego zakończenia postępowania. Po upływie tych okresów nagrania zawierające dane osobowe, podlegają zniszczeniu.

m) za dobrowolną zgodą w celu weryfikacji wniosku o wydanie identyfikatora, celem realizacji przepisów Regulaminu określającego zasady wjazdu i parkowania oraz zasady stosowania identyfikatorów uprawniających do parkowania pojazdów na terenach będących w Zarządzie Spółdzielni Mieszkaniowej do momentu wycofania.

n) za dobrowolną zgodą w celu zamieszczenia podstawowych danych identyfikacyjnych na listach domofonowych/spisie lokatorów do momentu wycofania zgody.

o) dane użytkowników systemu Marshal w związku z udostępnieniem konta w serwisie przez sieć Internet z poziomu przeglądarki internetowej przetwarzamy na podstawie Pani \ Pana dobrowolnej zgody przez okres korzystania z konta w czasie posiadania tytułu prawnego do lokalu, lub do momentu wycofania zgody. Logując się do systemu Marshal ma Pani/Pan dostęp do wysokości opłat czynszowych i eksploatacyjnych dotyczących mieszkania bądź lokalu użytkowego, salda oraz terminów płatności i dokonanych wpłat.

C. Zasada proporcjonalności

1. Zbierane dane osobowe winny być adekwatne, stosowne oraz ograniczone do danych niezbędnych do celów, dla których są przetwarzane. Administrator Danych Osobowych może zbierać i przetwarzać tylko takiego rodzaju dane, które są konieczne ze względu na cel zbierania danych w momencie ich zbierania.
2. Zbieranie innych danych (które mogłyby np. okazać się użyteczne w przyszłości) jest niedopuszczalne.

D. Zasada prawidłowości

1. Dane osobowe winny być zgodne ze stanem faktycznym, prawidłowe i aktualne.
2. W przypadku gdy biorąc pod uwagę cel przetwarzania danych osobowych okaże się, iż dane osobowe są nieprawidłowe, winny one zostać niezwłocznie sprostowane lub usunięte.

E. Zasada ograniczenia czasowego

1. Dane osobowe winny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla których dane te są przetwarzane.
2. W przypadku gdy nie jest możliwe określenie okresu przechowywania danych osobowych na podstawie obowiązujących przepisów lub aktów wewnętrznych Administratora Danych Osobowych, okres przechowywania ustala Administrator Danych Osobowych przy zachowaniu odpowiedniej równowagi między prawami jednostki wynikającymi z obowiązujących przepisów prawa, a własnymi i uzasadnionymi potrzebami związanymi z przetwarzaniem danych i osiągnięciem celów przetwarzania.
3. Postanowienie z ust. 1 nie ma zastosowania, gdy dane osobowe są przetwarzane wyłącznie do celów archiwalnych w interesie publicznym lub do celów statystycznych, pod warunkiem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.

F. Zasada bezpieczeństwa

1. Administrator Danych Osobowych obowiązany jest wdrożyć odpowiednie środki techniczne lub organizacyjne, odpowiednie do ryzyka naruszenia praw lub wolności osób fizycznych o różnym stopniu prawdopodobieństwa ich wystąpienia oraz wadze zagrożenia, celem zapewnienia integralności, poufności oraz dostępności danych osobowych.
2. Organizacyjne, techniczne oraz informatyczne środki ochrony informacji i danych osobowych wprowadzane są przez Administratora Danych Osobowych, celem zapobieżenia ryzyku związanemu z naruszeniem danych osobowych wskutek:
   a) sytuacji losowych (np. pożaru, zalania, katastrofy budowlanej),
   b) niewłaściwych parametrów środowiska, zakłócających pracę sprzętu komputerowego (np. nadmierna wilgoć lub wysoka temperatura),
   c) działań lub zaniechań pracowników, stanowiących naruszenie zasad i procedur ochrony danych osobowych,
   d) awarii sprzętu komputerowego lub oprogramowania, wskazujące na umyślne naruszenie ochrony danych osobowych,
   e) celowego lub przypadkowego rozproszenia danych osobowych w Internecie, z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego,
   f) wystąpienia katastrof naturalnych,
   g) infekcji systemów informatycznych,
   h) włamań do systemów informatycznych,
   i) przerw i zakłóceń w działaniu systemów informatycznych i innych.
3. Środki techniczne i organizacyjne, o których mowa powyżej obejmują w szczególności:
   a) stosowanie pseudonimizacji i szyfrowania danych osobowych,
   b) zdolność do nieprzerwanego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w przypadku wystąpienia incydentu fizycznego lub technicznego,
   d) regularne kontrolowanie skuteczności stosowanych środków.

G. Zasada domyślnej ochrony danych i ochrony danych w fazie projektowania

1. Administrator Danych Osobowych zapewnia realizację domyślnej ochrony danych osobowych, co oznacza iż przetwarzane są tylko te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Domyślna ochrona danych osobowych dotyczy następujących obszarów:
   a) ilości zbieranych danych osobowych,
   b) zakresu przetwarzania danych osobowych,
   c) okresu przechowywania danych osobowych,
   d) dostępności do danych osobowych,
   e) ograniczenia dostępu do danych osobowych.
2. Celem zapewnienia realizacji przedmiotowej zasady, Administrator Danych Osobowych na etapie projektowania nowych procedur, pojawienia się nowych procesów przetwarzania, wyboru nowych technologii dotyczących przetwarzania danych osobowych, będzie stosował odpowiednie środki techniczne, organizacyjne, stosowne do ryzyka naruszenia praw i wolności osób, których dane dotyczą.

H. Zasada integralności i poufności

Dane osobowe winny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

I. Zasada rozliczalności.

Administrator Danych Osobowych w osobie Prezesa Zarządu jest odpowiedzialny za przestrzeganie wyżej opisanych zasad i musi być w stanie wykazać ich wdrożenie i przestrzeganie.

IV. PRAWA OSÓB

Administrator Danych Osobowych zapewnia poufność, dostępność, integralność oraz rozliczalność przetwarzanych danych osobowych, poprzez zastosowanie niezbędnych środków organizacyjnych oraz technicznych.

Dobór powyższych środków ma na celu obniżenie poziomu ryzyka wystąpienia incydentów, związanych z bezpieczeństwem przetwarzania danych osobowych, do poziomu akceptowalnego przez Administratora Danych Osobowych.

Wprowadzenie przedmiotowych środków, zostało poprzedzone przeprowadzeniem analizy kosztów ich wdrożenia w odniesieniu do stopnia bezpieczeństwa przetwarzania danych osobowych, jaki Administrator Danych Osobowych zamierza osiągnąć po ich wdrożeniu.

A. W ramach grupy środków organizacyjnych wprowadza się w szczególności:

1) ewidencję upoważnień do przetwarzania danych osobowych, przy czym upoważnienia do przetwarzania danych osobowych winny być wydawane każdemu pracownikowi zgodnie z zakresem jego obowiązków;
2) szkolenia prowadzone dla osób upoważnionych obejmujące przepisy prawa powszechnie obowiązującego, wewnętrzne regulacje Administratora oraz wynikające z nich zasady bezpiecznego przetwarzania danych osobowych, w tym w formie e-learningowej, o której mowa w dziale VIII a niniejszej Polityki;

3) oświadczenia o zachowaniu w poufności danych osobowych i sposobów zabezpieczenia danych, które są zbierane od osób upoważnionych do przetwarzania danych osobowych;
4) monitorowanie przez Administratora Danych Osobowych przestrzegania niniejszej Polityki Spółdzielni Mieszkaniowej;
5) nadzór środowiska informatycznego;
6) umowy powierzenia w rozumieniu art. 28 ust. 3 RODO, zawierane z podmiotami przetwarzającymi dane w imieniu Administratora Danych Osobowych;
7) rejestr czynności przetwarzania danych osobowych zgodnie z art. 30 RODO;
8) zasadę, zgodnie z którą osoby trzecie przebywają w obszarze przetwarzania danych wyłącznie w obecności osoby upoważnionej. Osoby trzecie mogą w wyjątkowych okolicznościach przebywać bez obecności osoby upoważnionej - w obszarze przetwarzania danych - po uprzednim wydaniu na to zgody przez Administratora Danych Osobowych.

B. W ramach grupy środków technicznych, wprowadza się w szczególności:

1) zabezpieczenia techniczne zapewniające poufność przetwarzanych danych osobowych:
   a) obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych poprzez zastosowanie zamków patentowych i kodów dostępu;
   b) dane osobowe przetrzymywane w formie papierowej są przechowywane w zamykanych szafkach, szafach lub szufladach;
   c) pracownicy zobowiązani są do stosowania „polityki czystego biurka", poprzez umieszczanie dokumentów i nośników informacji w biurkach lub szafach zamykanych na klucz;
   d) pracownicy zobowiązani są do niszczenia na bieżąco dokumentacji roboczej lub tymczasowej zawierającej dane osobowe, po ustaniu celu jej przetwarzania;
   e) pracownicy zobowiązani są do przemieszczania dokumentacji zawierającej dane osobowe w sposób zabezpieczający ją przed zniszczeniem, utratą lub dostępem do niej osoby nieupoważnionej;
   f) dokumentacja zawierająca dane osobowe lub informacje podlega archiwizacji, zgodnie z powszechnie obowiązującymi przepisami;
   g) dostęp do danych w systemie informatycznym możliwy wyłącznie po uwierzytelnieniu użytkownika;
   h) hasła są zmieniane przez użytkowników nie rzadziej niż co 90 dni, jeżeli system nie wymusza tego automatycznie;
   i) na stacjach roboczych, za pomocą których są przetwarzane dane osobowe, instaluje się oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów;
   j) szyfrowanie nośników danych;
   k) monitorowanie działania systemu informatycznego;
   l) logiczna i fizyczna separacja sieci;
   m) logiczny dostęp do danych osobowych z sieci publicznej jest ograniczony poprzez zastosowanie zapory która chroni ona wszystkie systemy informatyczne przed nieuprawnionym dostępem i atakami z zewnątrz.
2) zabezpieczenia techniczne zapewniające integralność przetwarzanych danych osobowych:

a) ochrona przed nieautoryzowanym dostępem;
b) na stacjach roboczych, za pomocą których są przetwarzane dane osobowe, instaluje się oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów;
c) awaryjne podtrzymywanie zasilania serwerów;
d) właściwe okablowanie sieci;
e) cykliczna weryfikacja integralności baz danych poprzez odtwarzanie danych zawartych na kopiach zapasowych.

3) zabezpieczenia techniczne zapewniające rozliczalność przetwarzanych danych osobowych:
a) dostęp do danych w systemie informatycznym możliwy wyłącznie po uwierzytelnieniu użytkownika;
b) awaryjne podtrzymywanie zasilania serwerów;
c) zapis zdarzeń w systemach informatycznych.

C. Przetwarzanie danych osobowych poza obszarem przetwarzania dopuszczalne jest wyłącznie po spełnieniu poniższych przesłanek:

1. złożeniu wniosku o wyrażenie zgody na pracę z wykorzystaniem elektronicznych urządzeń przenośnych stanowiących własność Spółdzielni mieszkaniowej stanowiącej załącznik do Instrukcji zarządzania siecią i systemami informatycznymi, uzyskaniu zgody Administratora Danych Osobowych oraz zachowaniu szczególnej ostrożności podczas transportu, przechowania i użytkowania nośników zawierających dane osobowe;
2. zakaz pozostawiania nośników zawierających dane osobowe w sposób umożliwiający dostęp do nich osobom nieupoważnionym;
3. wykorzystywaniu nośników zawierających dane osobowe wyłącznie w celach służbowych;
4. regulacje dotyczące zdalnego dostępu oraz wynoszenia komputerów służbowych i innych elektronicznych urządzeń przenośnych poza siedzibę Spółdzielni Mieszkaniowej, znajdują się w Instrukcji zarządzania siecią i systemami informatycznymi w Spółdzielni Mieszkaniowej.

D. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1. likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie;
3. naprawy – pozbawia się wcześniej zapisu tych danych w sposób umożliwiający ich odzyskanie.

V. OBSZAR PRZETWARZANIA

1. Dane osobowe przetwarzane są w Spółdzielni Mieszkaniowej w:
a) w wersji elektronicznej:
I. w sieci komputerowej,
II. w systemach informatycznych,
III. w systemach pocztowych,
b) w wersji papierowej – w zbiorach papierowych.

2. Zasady przetwarzania danych osobowych w wersji elektronicznej określa Polityka Bezpieczeństwa Informacji oraz Regulamin monitoringu wizyjnego w odniesieniu do danych osobowych utrwalanych za pomocą systemu nadzoru wizyjnego.
3. Przetwarzanie danych osobowych odbywa się w obszarze przetwarzania wyznaczonym przez Administratora Danych Osobowych.
4. Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych prowadzi Administrator Danych Osobowych.
5. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych, poza obszarem przetwarzania, może nastąpić wyłącznie za zgodą Administratora Danych Osobowych.

VI. STRUKTURA

1. Administrator Danych Osobowych reprezentowany przez Prezesa Zarządu lub w czasie jego nieobecności V-ce Prezesa Zarządu wykonuje zadania z zakresu danych osobowych oraz sprawuje nadzór nad ich wykonaniem przez podległych mu pracowników, zleceniobiorców, instytucji i firm współpracujących ze Spółdzielnią.
2. Prezes Zarządu, V-ce Prezes Zarządu stosownie do zakresu realizowanych przez nich zadań statutowych wykonuje uprawnienia i obowiązki Administratora Danych Osobowych w zakresie wydawania upoważnień do przetwarzania danych osobowych i zawierania umów powierzenia przetwarzania danych osobowych oraz nadzoru nad przetwarzaniem danych osobowych w podległych im działów, celem zapewnienia bezpieczeństwa danych osobowych.

Do zadań Administratora Danych Osobowych należy przede wszystkim:

a) zapewnienia bezpieczeństwa i ochrony danych osobowych,
b) zapewnienie przestrzegania obowiązujących przepisów w zakresie ochrony danych osobowych oraz postanowień niniejszej Polityki w Spółdzielni Mieszkaniowej,
c) nadawanie upoważnień do przetwarzania danych osobowych, w tym upoważnień do przetwarzania danych osobowych, o których mowa w art. 9 i 10 RODO, nadawanych na podstawie przepisów odrębnych, tj. ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, oraz kodeks cywilny.
d) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
e) sprawowanie nadzoru nad bezpieczeństwem danych osobowych w Spółdzielni,
f) bieżące informowanie pracowników i osób współpracujących o ciążących na nich obowiązkach związanych z ochroną danych osobowych oraz udzielanie im porad w tym zakresie,
g) prowadzenie rejestru czynności przetwarzania oraz rejestru kategorii przetwarzania,
h) współpraca z Prezesem Urzędu Ochrony Danych Osobowych,
i) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych oraz prowadzenie uprzednich konsultacji, o których mowa w art. 36 RODO, oraz prowadzenie konsultacji we wszelkich innych sprawach.
j) administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem (w tym nadzór nad ich konfiguracją)

k) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych,
l) współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego,
m) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
n) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji poprzez analizę dokonanych naruszeń i próbę zapobiegnięciu ich w przyszłości,
o) przyznawanie praw dostępu do systemu informatycznego upoważnionym pracownikom, członkom,
p) prowadzenie ewidencji osób, którym nadano prawa dostępu do systemu informatycznego,
q) usprawnienie procedur bezpieczeństwa i standardów zabezpieczeń,
r) zarządzanie licencjami i procedurami ich dotyczącymi,
s) prowadzenie profilaktyki antywirusowej.
t) oraz inne wynikające z przepisów prawa polskiego i europejskiego w zakresie Ochrony Danych Osobowych.

VII. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby upoważnione do przetwarzania danych osobowych przez Administratora Danych Osobowych,
2. Zakres upoważnienia do przetwarzania danych osobowych jest adekwatny do zakresu wykonywanych zadań i realizowanych czynności zleconych przez Administratora Danych Osobowych.
3. Każda osoba w Spółdzielni mieszkaniowej przetwarza dane wyłącznie na podstawie otrzymanego upoważnienia wydanego przez Administratora Danych Osobowych, wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do niniejszej Polityki.
4. Dostęp do danych osobowych może uzyskać wyłącznie osoba upoważniona, która zobowiązała się do zachowania tych danych w poufności. Wzór oświadczenia o zachowaniu w poufności stanowi załącznik nr 2 do niniejszej Polityki.
4a. Do przetwarzania danych osobowych, o których mowa w art. 9 RODO, tj. danych osobowych szczególnych kategorii, dotyczących osób ubiegających się o zatrudnienie lub pracowników, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych, wydane na podstawie art. 22^{1b} § 3 ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy, zgodnie ze wzorem stanowiącym załącznik nr 1a do niniejszej Polityki. Osoby dopuszczone do przetwarzania takich danych są zobowiązane do zachowania ich w tajemnicy.
4b. Do przetwarzania danych osobowych dotyczących zdrowia, w rozumieniu RODO, o których mowa w ustawie z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych, oraz przepisów BHP, zgodnie ze wzorem stanowiącym załącznik nr 1b do niniejszej Polityki. Osoby dopuszczone do przetwarzania takich danych są zobowiązane do zachowania ich w tajemnicy.
5. Każda osoba otrzymująca upoważnienie do przetwarzania danych osobowych obowiązana jest zapoznać się z zasadami ochrony danych osobowych, w tym w szczególności z postanowieniami niniejszej Polityki oraz odbyć szkolenie z zakresu ochrony danych osobowych, o którym mowa w rozdziale VIII a niniejszej Polityki.
6. Osoby upoważnione do przetwarzania danych osobowych są uprawnione do przetwarzania danych osobowych wyłącznie w zakresie nadanego im upoważnienia.

VIII. PROCEDURA NADAWANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważnienia do przetwarzania danych osobowych nadają osoby wskazane w niniejszej polityce tj. Prezes Zarządu lub w przypadku jego nieobecności V-ce Prezes Zarządu.
2. Upoważnienia dla pracowników wydawane są w dwóch egzemplarzach, jeden egzemplarz otrzymuje osoba upoważniona, a drugi przechowywany jest aktach osobowych/teczce aktowej (dla osób powołanych oraz z wyboru).
3. Przed odebraniem upoważnienia do przetwarzania danych osobowych których wzory stanowią załączniki nr 1a, 1b każda osoba upoważniona zobowiązana jest do podpisania oświadczenia o zachowaniu w poufności powierzonych jej danych osobowych, stanowiącego załącznik nr 2 do niniejszej Polityki. Oświadczenie, o którym mowa w zdaniu pierwszym przygotowuje się w aktach osobowych.
4. Wygaśnięcie wszystkich nadanych upoważnień do przetwarzania danych osobowych następuje z chwilą rozwiązania lub wygaśnięcia stosunku pracy lub z chwilą ustania innego stosunku prawnego lub zakończenia pełnienia funkcji, w ramach której nadane zostało upoważnienie do przetwarzania danych.
5. Administrator Danych Osobowych może wycofać upoważnienie do przetwarzania danych osobowych w razie stwierdzenia zawinionego naruszenia ochrony danych osobowych.
6. Ewidencję pracowników upoważnionych do przetwarzania danych osobowych prowadzi Administrator Danych Osobowych.

VIII a. SZKOLENIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

1. Każda osoba otrzymująca upoważnienie do przetwarzania danych osobowych, zobowiązana jest do odbycia szkolenia z zakresu ochrony danych osobowych, prowadzonego przez Administratora Danych Osobowych.
2. Szkolenia odbywają się w formie e-learningu.
3. Osoba otrzymująca upoważnienie do przetwarzania danych osobowych odbiera poprzez elektroniczną skrzynkę pocztową, przekazany przez Administratora Danych Osobowych, dedykowany dla niej dostęp do materiału szkoleniowego.
4. Osoba upoważniona do przetwarzania danych jest zobowiązana odbyć szkolenie w terminie 14 dni od dnia otrzymania dostępu do materiału szkoleniowego.
5. Ukończenie szkolenia potwierdzone zostaje imiennym certyfikatem.
6. Certyfikaty dla pracowników wydawane są w dwóch egzemplarzach. Jeden egzemplarz, niezwłocznie po ukończeniu szkolenia, udostępniony jest pracownikowi do wydruku przez aplikację szkoleniową, a drugi przechowywany jest w aktach osobowych.

IX. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Spółdzielnia mieszkaniowa z podmiotami (współpracującymi) przetwarzającymi dane osobowe w imieniu Administratora Danych Osobowych zawiera umowy powierzenia przetwarzania danych osobowych.
2. Do umów, porozumień itp. które związane są z powierzeniem danych osobowych podmiotom zewnętrznym Administrator Danych Osobowych przygotowuje do umowy podstawowej dodatkowo umowę powierzenia danych osobowych. Zawarcie odrębnej umowy nie jest konieczne, jeśli w umowie podstawowej zostaną zawarte wszystkie niezbędne zapisy dotyczące kwestii powierzenia danych osobowych.

3. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszej Polityki.
4. Wykaz podmiotów przetwarzających prowadzony jest zgodnie ze wzorem stanowiącym załącznik nr 4 do niniejszej Polityki.

X. ZAPEWNIENIE REALIZACJI PRAW I WOLNOŚCI OSÓB, KTÓRYCH DANE DOTYCZĄ

Administrator Danych Osobowych ma świadomość, że zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach.
Administrator zapewniając realizację praw i wolności osób, których dane dotyczą, podejmuje odpowiednie, środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania.
Zapewniając realizację praw i wolności osób, których dane dotyczą Administrator Danych Osobowych ustala następujące zasady:

1. Informacji, o których mowa w art. 13 i 14 RODO udziela się na piśmie lub w inny sposób, w tym elektronicznie.
2. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile potwierdzi się tożsamość osoby, której dane dotyczą. Potwierdzenie tożsamości w formie elektronicznej lub papierowej następuje poprzez weryfikację co najmniej dwóch dodatkowych danych osobowych (poza imieniem i nazwiskiem). Niniejsze postanowienie nie dotyczy zapytań skierowanych przez pracowników Spółdzielni Mieszkaniowej przy użyciu służbowej poczty elektronicznej.
3. Informacji, o których mowa w art. 13 RODO udziela się podczas pozyskiwania danych osobowych.
4. Informacji, o których mowa w art. 14 RODO udziela się bez zbędnej zwłoki – nie później niż w terminie miesiąca od otrzymania danych osobowych, z zastrzeżeniem postanowienia art. 14 ust. 3 lit. b i c RODO.
5. Osobie, której dane dotyczą, udziela się informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–21 RODO.
6. W przypadku przetwarzania niewymagającego identyfikacji, tam gdzie Administrator Danych Osobowych nie jest w stanie zidentyfikować podmiotu danych, Administrator Danych Osobowych w miarę możliwości informuje tą osobę, iż nie mają zastosowania art. 15-20 RODO, chyba że osoba której dane dotyczą dostarczy dodatkowych informacji pozwalających na jej identyfikację.
7. W przypadku pozyskiwania danych bezpośrednio od osoby, której dane dotyczą, informuje się tą osobę o przetwarzaniu jej danych osobowych, zgodnie ze wzorem stanowiącym załącznik nr 5 do niniejszej Polityki.
8. W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, przedstawia się danej osobie klauzule informacyjne, zgodnie ze wzorem stanowiącym załącznik nr 6 do niniejszej Polityki.
9. Jeżeli Administrator Danych Osobowych planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane zostały pozyskane, przed dalszym przetwarzaniem winien poinformować osobę której dane dotyczą o tym innym celu oraz udzielić jej wszelkich innych stosownych informacji, o których mowa odpowiednio w ust. 7 lub 8 powyżej.

10. Administrator Danych Osobowych bez zbędnej zwłoki, informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator Danych Osobowych informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
11. Administrator zapewnia realizację następujących praw i wolności osób, których dane dotyczą:

Prawo dostępu przysługujące osobie, której dane dotyczą

Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora Danych Osobowych potwierdzenia, czy jej dane osobowe są przetwarzane, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz uzyskania informacji, określających:

- cele przetwarzania;
- kategorie odnośnych danych osobowych;
- informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawie do żądania od Administratora Danych Osobowych sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Administrator Danych Osobowych dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu.
Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator Danych Osobowych może pobrać opłatę w wysokości odpowiadającej administracyjnym kosztom jej wytworzenia.
Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną równocześnie nie wskazując formy ich przekazania, informacji udziela się za pośrednictwem firmowej poczty elektronicznej.

Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od Administratora Danych Osobowych niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Prawo do bycia zapomnianym

Osoba, której dane dotyczą, ma prawo żądania od Administratora Danych Osobowych niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator Danych Osobowych ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania jej danych osobowych;
- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega Administrator Danych Osobowych;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

Jeżeli Administrator Danych Osobowych upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Prawo do usunięcia danych nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega Administrator Danych Osobowych lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych Osobowych;
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że realizacja prawa do bycia zapomnianym uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
- do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą, ma prawo żądania od Administratora Danych Osobowych ograniczenia przetwarzania w następujących przypadkach:

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi Danych Osobowych sprawdzić prawidłowość tych danych;
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- Administrator Danych Osobowych nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

- osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora Ochrony Danych są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Jeżeli zgodnie z żądaniem przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Przed uchyleniem ograniczenia przetwarzania Administrator Danych Osobowych informuje o tym osobę, której dane dotyczą, która żądała ograniczenia przetwarzania.

Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, dane osobowe jej dotyczące, które dostarczyła Administratorowi Danych Osobowych, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora Danych Osobowych, któremu dostarczono te dane osobowe, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy; oraz
b) przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora Danych Osobowych bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku prawa do bycia zapomnianym. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Administrator Danych Osobowych odmawia realizacji prawa do przenoszenia danych w sytuacji, gdy realizacja tego prawa może niekorzystnie wpływać na prawa i wolności innych osób.

Prawo do sprzeciwu

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, gdy:

- przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych Osobowych;
- przetwarzanie danych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych Osobowych, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Administratorowi Danych Osobowych nie wolno już przetwarzać danych osobowych w sytuacji skorzystania z prawa do sprzeciwu, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

XI. PROCEDURA UDOSTĘPNIENIA DANYCH

Celem niniejszej procedury jest określenie zasad udostępniania danych osobom, których dane dotyczą, a także organom publicznym, które wnioskują o udostępnienie danych osobowych w ramach prowadzonego przez te organy postępowania.

1. Dane osobowe udostępnia się na pisemny wniosek, chyba że obowiązujące przepisy stanowią inaczej.
2. W przypadku wniosku o udostępnienie danych, każda osoba, do której wpłynie taki wniosek, a która ma uzasadnione wątpliwości czy udostępnienie danych będzie zgodne z przepisami prawa, jest zobowiązana przekazać wniosek do Inspektora Ochrony Danych.
3. Administrator Danych Osobowych rozpatruje przekazany wniosek oraz ustala czy wniosek o udostępnienie:
    a) wystarczająco identyfikuje osobę, której dane mają być udostępnione;
    b) posiada odpowiednią podstawę prawną udostępnienia danych;
    c) określa zakres żądanych danych osobowych.
4. Administrator Danych Osobowych ocenia, czy można legalnie udostępnić dane osobowe wnioskodawcy.
5. W razie braków formalnych wniosku o udostępnienie danych osobowych, Administrator Danych Osobowych zwraca się do wnioskodawcy o ich usunięcie we wskazanym terminie pod rygorem pozostawienia wniosku bez rozpoznania.
6. Po uzyskaniu pozytywnej opinii od Inspektora Ochrony Danych (jeśli taka osoba jest wyznaczona) w przedmiocie dopuszczalności udostępnienia danych osobowych, Administrator Danych Osobowych bez zbędnej zwłoki udostępnia dane osobowe.
7. Dane osobowe powinny być udostępniane w sposób zapewniający ich poufność wobec osób postronnych.
8. Po uzyskaniu negatywnej opinii Inspektora Ochrony Danych (jeśli taka osoba została wyznaczona) w przedmiocie dopuszczalności udostępnia danych osobowych, Administrator Danych Osobowych informuje wnioskodawcę o odmowie udostępnienia danych osobowych.

XII. INWENTARYZACJA

1. Administrator Danych Osobowych identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne oraz utrzymuje adekwatne mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych, Administrator Danych Osobowych postępuje zgodnie z zasadami przyjętymi w tym zakresie.
2. Administrator Danych Osobowych identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
3. Administrator Danych Osobowych identyfikuje przypadki, w których dokonuje profilowania przetwarzania danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, Administrator Danych Osobowych postępuje zgodnie z przyjętymi zasadami w tym zakresie.
4. Administrator Danych Osobowych identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

XIII. ANALIZA RYZYKA

1. Analiza ryzyka jest przeprowadzana przez Spółdzielnię Mieszkaniową Pracowników Wsk Pzl Kraków w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń, wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. W Spółdzielni mieszkaniowej analizę ryzyka w obszarze bezpieczeństwa informacji przeprowadza się systematycznie, stosownie do bieżących potrzeb, w każdym jednak przypadku nie rzadziej niż raz do roku.
2. W przypadku podjęcia przez Administratora Danych Osobowych decyzji o konieczności obniżenia ryzyka związanego z przetwarzaniem danych osobowych, wyznaczona zostanie lista zabezpieczeń do wdrożenia, termin realizacji oraz osoby odpowiedzialne za realizację przedmiotowego zadania.

XIV. NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Każdy pracownik zobowiązany jest do niezwłocznego powiadamiania o ryzyku wystąpienia lub wystąpieniu przypadku naruszenia ochrony danych osobowych (tzw. incydentu) swemu przełożonemu oraz Administratorowi Danych Osobowych.
2. W przypadku stwierdzenia wystąpienia ryzyka lub wystąpienia przypadku naruszenia ochrony danych osobowych Administrator Danych Osobowych prowadzi postępowanie wyjaśniające podczas którego:
   a) ustala czas, zakres i przyczyny oraz jego ewentualne skutki,
   b) działa na rzecz przywrócenia prawidłowego funkcjonowania Spółdzielni Mieszkaniowej
      po wystąpieniu incydentu,
   c) rekomenduje działania zapobiegawcze zmierzające do eliminacji podobnych zdarzeń w przyszłości lub minimalizacji strat w momencie ich zaistnienia,
   d) ustala osoby odpowiedzialne oraz inicjuje ewentualne działania dyscyplinarne.
3. Administrator Danych Osobowych obowiązany jest dokumentować wszystkie przypadki naruszenia ochrony danych osobowych.
4. Administrator Danych Osobowych prowadzi rejestr incydentów, zgodnie ze wzorem stanowiącym załącznik nr 7 do niniejszej Polityki.
5. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator Danych Osobowych niezwłocznie, nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych.
6. W przypadku gdy naruszenie danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych Osobowych zawiadamia osobę, której takie dane dotyczą, o zaistniałym naruszeniu.

XV. ZAŁĄCZNIKI

Integralną część niniejszej Polityki stanowią następujące załączniki:

Załącznik nr 1	- Wzory upoważnień (1, 1a i 1b),
Załącznik nr 2	- Wzór oświadczenia o zachowaniu w poufności,
Załącznik nr 3	- Wzór umowy powierzenia przetwarzania danych osobowych,
Załącznik nr 4	- Wykaz podmiotów przetwarzających dane osobowe w imieniu Administratora Danych Osobowych (4, 4a – klauzula informacyjna dla pozyskania danych od osoby której dane dotyczą (współadministrowa-

	nie), 4b – klauzula informacyjna w przypadku pozyskania danych w inny sposób (współadministrowanie))
Załącznik nr 5	- Wzór klauzuli informacyjnej dla osoby od której pozyskiwane są jej dane osobowe,
Załącznik nr 6	- Wzór klauzuli informacyjnej w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą
Załącznik nr 7	- Rejestr incydentów
Załącznik nr 8	– Wykaz zbiorów danych wraz z procesami przetwarzania danych osobowych

.....

Podpis Przewodniczącego Rady Nadzorczej

.....

Podpis Z-cy Przewodniczącego Rady Nadzorczej

.....

Podpis Sekretarza Rady Nadzorczej

.....

Podpis Rady Nadzorczej

.....

Podpis Rady Nadzorczej

.....

Podpis Rady Nadzorczej