**Polityka Bezpieczeństwa**

**Danych Osobowych**

**w Śródmiejskiej Spółdzielni Mieszkaniowej**

**w upadłości likwidacyjnej**

**POSTANOWIENIA OGÓLNE**

**§ 1**

Polityka Bezpieczeństwa jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu danych osobowych zarówno w sposób zautomatyzowany poza zbiorem danych, jak również
w zbiorach danych, w toku działalności prowadzonej przez Śródmiejską Spółdzielnię Mieszkaniową w upadłości likwidacyjnej, a w szczególności określa środki techniczne i organizacyjne wdrożone przez Śródmiejską Spółdzielnię Mieszkaniową w upadłości likwidacyjnej w celu zapewnienia maksymalnej ochrony danych osobowych zgodnie z obowiązującymi przepisami, a w szczególności Rozporządzeniem Parlamentu Europejskiego i Rady Unii Europejskiej 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).

**§ 2**

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
2. **Spółdzielnia** – Śródmiejska Spółdzielnia Mieszkaniowa w upadłości likwidacyjnej w Warszawie przy Al. 3 Maja 12. Spółdzielnia jest jednocześnie administratorem danych osobowych w rozumieniu art. 4 pkt. 7 RODO, tj. podmiotem, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
3. **Inspektor Ochrony Danych** – osoba wyznaczona przez Śródmiejską Spółdzielnię Mieszkaniową w upadłości likwidacyjnej na podstawie art. 37 ust. 4 RODO, nadzorująca przestrzeganie zasad ochrony danych osobowych w Śródmiejskiej Spółdzielni Mieszkaniowej w upadłości likwidacyjnej oraz realizująca zadania przewidziane w art. 39 RODO.
4. **Administrator Systemu Informatycznego** – osoba odpowiedzialna za zapewnienie ciągłości i poprawności działania systemu lub aplikacji.
5. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
6. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
7. **Przetwarzanie danych osobowych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
8. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
9. **Usuwanie danych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
10. **Użytkownik** – osoba upoważniona do przetwarzania danych osobowych przez Śródmiejską Spółdzielnię Mieszkaniową w upadłości likwidacyjnej.
11. **Zabezpieczenie systemu informatycznego** – wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.
12. **Zgoda osoby, której dane dotyczą** – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

**ZAKRES STOSOWANIA**

**§ 3**

1. W Spółdzielni przetwarzane są informacje służące realizacji celu działania Spółdzielni, określonego w ustawie, do którego należy zaspokajanie potrzeb mieszkaniowych członków oraz ich rodzin, jak również innych potrzeb przez dostarczanie samodzielnych lokali mieszkalnych, domów jednorodzinnych, a także lokali o innym przeznaczeniu poprzez:

* budowanie lub nabywanie budynków w celu ustanowienia na rzecz członków spółdzielczego lokatorskiego prawa do lokali mieszkalnych znajdujących się w tych budynkach;
* budowanie lub nabywanie budynków w celu ustanowienia na rzecz członków odrębnej własności lokali mieszkalnych lub lokali o innym przeznaczeniu, a także ułamkowego udziału we współwłasności w garażach wielostanowiskowych;
* budowanie lub nabywanie domów jednorodzinnych w celu przeniesienia na rzecz członków własności tych domów;
* udzielanie pomocy członkom w budowie budynków mieszkalnych lub domów jednorodzinnych;
* budowanie lub nabywanie budynków oraz innych urządzeń gospodarczych, pomocniczych i rekreacyjnych niezbędnych dla realizacji zadań Spółdzielni lub w celu wynajmowania lub sprzedaży lokali mieszkalnych lub lokali o innym przeznaczeniu znajdujących się w tych budynkach;
* utrzymywanie nieruchomości wraz z infrastrukturą stanowiącą własność Spółdzielni i własność jej członków w należytym stanie technicznym;
* nabywanie potrzebnych Spółdzielni terenów;
* zarządzanie nieruchomościami stanowiącymi własność Spółdzielni oraz własność jej członków, jak również zarządzanie nieruchomościami nie stanowiącymi jej mienia lub mienia jej członków na podstawie umowy zawartej z właścicielem bądź współwłaścicielami tej nieruchomości;
* prowadzenie gospodarki zasobami mieszkaniowymi;
* prowadzenie działalności gospodarczej, w tym tworzenie wydzielonych zakładów związanych bezpośrednio z realizacją celów Spółdzielni.

2.Informacje te są przetwarzane i składowane zarówno w postaci dokumentacji papierowej jak i elektronicznej.

3.Załączniki doPolityki Bezpieczeństwa stanowią dokumenty odzwierciadlające wprowadzone zabezpieczenia techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych.

**§ 4**

Politykę Bezpieczeństwa stosuje się w szczególności do:

1. danych osobowych przetwarzanych w zbiorach danych,
2. danych osobowych gromadzonych w związku z działalnością Spółdzielni,
3. wszystkich informacji dotyczących danych pracowników i współpracowników Spółdzielni, w tym danych osobowych tych osób i treści zawieranych z nimi umów
o pracę i umów cywilnoprawnych,
4. wszystkich informacji dotyczących członków Spółdzielni,
5. wszystkich informacji dotyczących właścicieli lokali (lub domów jednorodzinnych) położonych w budynkach wchodzących w skład zasobów Spółdzielni lub którymi Spółdzielnia zarządza,
6. wszystkich informacji dotyczących najemców lokali wchodzących w skład zasobów Spółdzielni,
7. wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
8. wszystkich danych osobowych kontrahentów Spółdzielni oraz osób wyznaczonych przez kontrahentów do kontaktów ze Spółdzielnią,
9. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.
10. rejestru osób upoważnionych do przetwarzania danych osobowych,
11. innych dokumentów zawierających dane osobowe.

**§ 5**

1. Zakresy ochrony danych osobowych określone przez Politykę Bezpieczeństwa mają zastosowanie do systemu informatycznego Spółdzielni, w którym są przetwarzane dane osobowe.

2. Do stosowania zasad określonych przez Politykę Bezpieczeństwa zobowiązane są wszystkie osoby dopuszczone przez Spółdzielnię do przetwarzania danych osobowych, co obejmuje
w szczególności pracowników Spółdzielni, jego współpracowników, konsultantów, stażystów, wolontariuszy oraz inne osoby mające dostęp do danych osobowych.

**PODSTAWOWE ZASADY PRZY PRZETWARZANIU DANYCH OSOBOWYCH**

**§ 6**

1. Obszarem przetwarzania danych osobowych w Spółdzielni są pomieszczenia w siedzibie Spółdzielni położone w budynku przy Al. 3 Maja 12 w Warszawie oraz w biurze Administracji przy ul. Grzybowskiej 9, do których osoby nieupoważnione do przetwarzania danych osobowych przez Spółdzielnię nie mają wstępu.

2. Przetwarzanie danych osobowych następuje z użyciem sprzętu komputerowego, zabezpieczonego odpowiednimi systemami antywirusowymi oraz zabezpieczonego przed nieuprawnionym dostępem loginem oraz hasłem składającym się z co najmniej 8 znaków,
w tym przynajmniej jednej dużej litery, jednej cyfry i jednego znaku specjalnego.

3. Przetwarzanie danych poza siedzibą Spółdzielni jest dopuszczalne, gdy osoba przetwarzająca dane zapewnia dozór osobisty nad sprzętem komputerowym lub innym nośnikiem danych uniemożliwiając nieuprawniony dostęp osób trzecich do danych osobowych.

**§ 7**

1. Przetwarzanie danych osobowych jest dopuszczalne jedynie w zakresie działania Spółdzielni.

2. Przetwarzanie danych osobowych przez Spółdzielnię następuje wyłącznie, gdy:

1. osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych osobowych,
2. przetwarzanie jest niezbędne do wykonania umowy zawartej ze Spółdzielnią, której stroną jest osoba, której dane dotyczą, lub podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy ze Spółdzielnią,
3. przetwarzanie jest niezbędne dla wypełnienia obowiązku prawnego ciążącego na Spółdzielni,
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,
6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Spółdzielnię lub przez stronę trzecią, 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.

3. Przetwarzanie na podstawie zgody jest dokonywane po uprzednim uzyskaniu od osoby, której dane dotyczą, oświadczenia obejmującego zgodę na przetwarzanie danych osobowych, przy której każdorazowo informuje się osoby, których dane dotyczą o prawie wycofania zgody w dowolnym momencie.

4. W Spółdzielni zabrania się przetwarzania następujących danych osobowych:

1. ujawniających pochodzenie rasowe lub etniczne,
2. ujawniających poglądy polityczne,
3. ujawniających przekonania religijne lub światopoglądowe,
4. ujawniających przynależność do związków zawodowych,
5. danych genetycznych,
6. danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej bez uprzedniego uzyskania pisemnej zgody tej osobyw,
7. danych dotyczących zdrowia, seksualności lub orientacji seksualnej,
8. danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie w/w danych będzie możliwe wyłącznie w przypadku spełnienia jednej z przesłanek legalizujących wskazanych w art. 9 ust. 2 RODO.

**§ 8**

W Spółdzielni dane osobowe są:

1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
4. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,
5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do osiągnięcia celów, w których dane są przetwarzane,
6. dane muszą 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.

**DEFINICJA BEZPIECZEŃSTWA INFORMACJI**

**§ 9**

1. Utrzymanie bezpieczeństwa przetwarzanych w Spółdzielni informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

2.Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji
i aplikacji:

* 1. Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy
	i współpracownicy mają dostęp do informacji;
	2. Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;
	3. Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
	4. Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania
	i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informatycznych.

**STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA**

**§ 10**

1. Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych danych osobowych.
2. Dokumenty do Polityki Bezpieczeństwa oraz sama Polityka Bezpieczeństwa będą regularnie poddawane przeglądom pod kątem ich skuteczności dla ochrony danych osobowych i w miarę potrzeb aktualizowane.

**DOSTĘP DO INFORMACJI**

**§ 11**

Wszystkie osoby, których rodzaj wykonywanej pracy lub zadań wiąże się z dostępem do danych osobowych, przed przystąpieniem do ich przetwarzania, są informowane i podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Spółdzielni zasad ochrony danych osobowych.

**§ 12**

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych określa zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

**§ 13**

1. Dane osobowe są przetwarzane wyłącznie przez osoby imiennie i pisemnie do tego upoważnione do tego przez Spółdzielnię ze wskazaniem zakresu upoważnienia.

2. Spółdzielnia prowadzi rejestr osób uprawnionych do przetwarzania danych osobowych, który zawiera:

1. imię i nazwisko osoby upoważnionej;
2. datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
3. identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

**§ 14**

W przypadku odwołania zgody na przetwarzanie danych przez osobę, której dane dotyczą, Spółdzielnia jest obowiązana do ich niezwłocznego usunięcia, chyba że dane nie mogą być usunięte, np. ze względu na obowiązujące przepisy.

**BEZPIECZEŃSTWO INFORMACJI**

**§ 15**

1. W Spółdzielni należy stosować następujące kategorie środków zabezpieczenia danych osobowych:

1. Zabezpieczenie fizyczne:
* pomieszczenia zamykane na klucz

szafy pancerne,

* szafy z zamkami.
1. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
* przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
* przetwarzanie danych przez wyznaczone do tego celu osoby,
* dokumenty zawierające dane osobowe zbędne do prowadzenia dalszych działań i które nie podlegają archiwizacji są niezwłocznie niszczone w sposób uniemożliwiający ich odczytanie.
1. Zabezpieczenie organizacyjne:
* osobami bezpośrednio odpowiedzialnymi za bezpieczeństwo danych są: użytkownicy, Administrator Systemu Informatycznego i Inspektor Ochrony Danych, a do czasu jego powołania – Koordynator ds. danych osobowych,
* Inspektor Ochrony Danych/Koordynator, Administrator Systemu Informatycznego na bieżąco kontrolują z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i obowiązującymi procedurami, pracę pracowników odpowiedzialnych za przetwarzanie danych osobowych oraz systemu informatycznego.
1. Zabezpieczenia informatyczne:

- Nie rzadziej niż raz na kwartał są prowadzone przez Inspektora Ochrony Danych/Koordynatora czynności sprawdzające stan bezpieczeństwa systemów informatycznych i przestrzegania zasad ochrony danych osobowych.

- W przypadkach wykrycia zaniedbań Inspektor Ochrony Danych, a do czasu jego powołania - Administrator Systemu Informatycznego, sporządza ich opis w formie pisemnej i niezwłocznie przedkłada Dyrektorowi.

**§ 16**

Ochronę danych osobowych w Spółdzielni należy realizować z wykorzystaniem następujących zabezpieczeń:

1. przyznawanie indywidualnych identyfikatorów,
2. zapewnienie wymuszania zmiany haseł;
3. odnotowania daty pierwszego wprowadzenia danych w systemie;
4. odnotowania identyfikatora użytkownika wprowadzającego dane;
5. odnotowania skorzystania przez osoby, których dane dotyczą, z praw przysługujących im na mocy art. 15-22 RODO;
6. odnotowania źródła danych, w przypadku zbierania danych nie od osoby, której dane dotyczą;
7. odnotowania informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia, a także informacji o użytkownikach, którzy udostępnili te dane;
8. zapewnienia możliwości sporządzenia i wydrukowania raportu zawierającego dane osobowe wraz z informacjami o historii przetwarzania danych.

**§ 17**

1. W ramach zabezpieczenia danych osobowych ochronie podlegają:

* 1. sprzęt komputerowy – serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne;
	2. oprogramowanie – kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne;
	3. dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie;
	4. hasła użytkowników;
	5. pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa;
	6. użytkownicy i administratorzy, którzy obsługują i używają system;
	7. dokumentacja – zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje itp.;
	8. wydruki;
	9. związana z przetwarzaniem danych osobowych dokumentacja papierowa, z której dane są wprowadzane do systemu informatycznego lub też funkcjonują niezależnie od niego.

**§ 18**

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych użytkownik jest zobowiązany niezwłocznie powiadomić o tym Spółdzielnię, w tym Inspektora Ochrony Danych, oraz podjąć działania minimalizujące naruszenie bezpieczeństwa ochrony danych osobowych, a także zabezpieczające przetwarzane przez Spółdzielnię dane osobowe.

2. Naruszenie bezpieczeństwa ochrony danych osobowych występuje w szczególności
w przypadku:

1. niewłaściwego zabezpieczenia fizycznego pomieszczeń, urządzeń i dokumentów,
2. niewłaściwego zabezpieczenia sprzętu, oprogramowania przed wyciekiem, kradzieżą
i utratą danych osobowych,
3. nieprzestrzegania zasad ochrony danych osobowych przez użytkowników,
4. pozostawienia danych osobowych niezabezpieczonych lub nieprzechowywanych
w zamykanych szafach.

3. W przypadku stwierdzenia wystąpienia naruszenia ochrony danych osobowych – w ramach postępowania wewnętrznego – Spółdzielnia:

1. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
2. dokonuje oceny możliwości ryzyka naruszenia praw lub wolności osób fizycznych,
3. podejmuje wszelkie niezbędne działania dla usunięcia naruszenia oraz jego skutków,
4. inicjuje ewentualne działania dyscyplinarne,
5. rekomenduje oraz wdraża działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
6. dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w sposób umożliwiające organowi nadzorczemu weryfikację przestrzegania przepisów obowiązujących w tym zakresie.

4. Z postępowania wewnętrznego Spółdzielnia sporządza protokół obejmujący wszystkie wymienione w ust. 3 elementy, który Spółdzielnia przechowuje w celu ewentualnego udostępnienia organowi nadzorczemu.

5. Niezależnie od opisanego w ust. 4 postępowania wewnętrznego, Spółdzielnia bez zbędnej zwłoki – w miarę możliwości, ale nie później niż w terminie 72 godzin po stwierdzeniu naruszenia ochrony danych osobowych – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin Spółdzielnia dołącza wyjaśnienie przyczyn opóźnienia.

6. W zgłoszeniu, o którym mowa w ust. 5, Spółdzielnia:

1. 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;
2. zawiera imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych;
3. opisuje możliwe konsekwencje naruszenia ochrony danych osobowych;
4. opisuje środki zastosowane lub proponowane przez Spółdzielnię w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środków
w celu zminimalizowania jego ewentualnych negatywnych skutków.

7. Spółdzielnia, stwierdziwszy naruszenie ochrony danych osobowych, każdorazowo dokonuje oceny możliwości ryzyka naruszenia praw lub wolności osób fizycznych, zamieszczając jej wynik w protokole, o którym mowa w ust. 4.

8. W przypadku stwierdzenia, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Spółdzielnia bez zbędnej zwłoki zawiadamia każdą osobę, której dane dotyczą, o takim naruszeniu, chyba że Spółdzielnia zastosowała następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

9. Zawiadomienie, o którym mowa w ust. 8, zostanie sporządzone przez Spółdzielnię w taki sposób, aby opisywało jasnym i prostym językiem charakter naruszenia ochrony danych osobowych, a ponadto zawierało oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji, opis możliwych konsekwencji naruszenia ochrony danych osobowych,
a także opis środków zastosowanych lub proponowanych przez Spółdzielnię w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

**§ 19**

1. Spółdzielnia wyznacza Inspektora Ochrony Danych, a do czasu jego powołania - Koordynatora, którego zadaniem będzie realizacja praw osób fizycznych, których dane są przetwarzane przez Spółdzielnię, wynikające z RODO.

W przypadku skorzystania przez osobę, której dane dotyczą, z jednego z następujących praw:

* prawa dostępu do danych,
* prawa do uzyskania kopii danych,
* prawa do sprostowania danych,
* prawa do usunięcia danych,
* prawa do ograniczenia przetwarzania danych,
* prawa do przenoszenia danych,
* prawa do sprzeciwu oraz
* prawa do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu,

które to prawa przysługują osobom fizycznym na mocy art. 15-22 RODO, osoba wyznaczona przez Spółdzielnię będzie miała obowiązek ustosunkować się do nich niezwłocznie, jednak nie później niż w terminie 2 tygodni, a następnie przekazać stanowisko do akceptacji Spółdzielni.

2. Spółdzielnia po przeanalizowaniu stanowiska Inspektora/Koordynatora niezwłocznie
- a w każdym razie w terminie miesiąca od otrzymania żądania - udzieli osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15-22 RODO.

3. W razie potrzeby termin Spółdzielnia przedłuży o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. Jednak w terminie miesiąca od otrzymania żądania Spółdzielnia poinformuje osobę, której dane dotyczą o takim przedłużeniu terminu,
z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

4. W przypadku, gdy Spółdzielnia nie podejmie działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

5. Osoba wyznaczona do realizacji praw wynikających z art. 15-22 RODO jest odpowiedzialna zarówno za sporządzanie pisemnych stanowisk Spółdzielni, które następnie będą podlegały akceptacji przez Spółdzielnię, jak i wszczynanie procedur koniecznych dla realizacji przez Spółdzielnię tych praw w ramach struktury organizacyjnej Spółdzielni.

6. Osoba wyznaczona do realizacji praw wynikających z art. 15-22 RODO prowadzi rejestr żądań osób fizycznych w tym zakresie, a także co miesiąc ma obowiązek złożenia Spółdzielni sprawozdań o podjętych w tym zakresie działaniach.

**§ 20**

1. W przypadku, gdy Spółdzielnia powierza innemu podmiotowi przetwarzanie danych, przed rozpoczęciem czynności powierzenia, Spółdzielnia zawiera stosowną umowę o powierzeniu przetwarzania danych osobowych.

2. Powierzenie przetwarzania danych innemu podmiotowi nastąpi wyłącznie na podstawie pisemnej umowy spełniającej warunki art. 28 ust. 3 RODO.

**ZARZĄDZANIE DANYMI OSOBOWYMI**

**§ 21**

1. Za bezpieczeństwo danych osobowych w Spółdzielni odpowiadają:
	1. Spółdzielnia jako administrator danych osobowych
	2. Inspektor Ochrony Danych, a do czasu jego powołania - Koordynator
	3. Administrator Systemu Informatycznego
2. W umowach zawieranych przez Spółdzielnię z podmiotami trzecimi winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych osobowych udostępnionych przez Spółdzielnię oraz do zachowania poufności.
3. Przy zawieraniu umów o pracę oraz o współpracy zawieranych przez Spółdzielnię
z pracownikami i współpracownikami wprowadza się postanowienia zobowiązujące do ochrony danych osobowych udostępnionych przez Spółdzielnię oraz do zachowania tajemnicy.

**§ 22**

1. Inspektor Ochrony Danych, a do czasu jego powołania – Koordynator, zobowiązany jest do przekazania pracownikom, współpracownikom i kontrahentom oraz członkom Spółdzielni i innym osobom, których dane są przetwarzane przez Spółdzielnię, informacji
o przetwarzaniu danych osobowych, które ich dotyczą.
2. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
	1. rejestr pracowników i współpracowników Spółdzielni upoważnionych do przetwarzania danych osobowych znajduje się u Inspektora Ochrony Danych;
	2. przetwarzać dane osobowe mogą jedynie pracownicy i współpracownicy, którzy zostali zapoznani z obowiązującymi zasadami dotyczącymi ochrony danych osobowych, przeszkoleni i posiadają upoważnienie przyznane przez Spółdzielnię;
	3. w czasie przetwarzania danych osobowych każda osoba upoważniona jest osobiście odpowiedzialna za bezpieczeństwo powierzonych jej danych;
	4. po zakończeniu przetwarzania danych (w tym na koniec każdego dnia pracy) osoba upoważniona winna należycie zabezpieczyć dane osobowe przed możliwością wglądu, bądź zmiany, przez osoby do tego celu nieupoważnione;
	5. przetwarzanie danych osobowych w Spółdzielni jest okresowo kontrolowane przez Inspektora Ochrony Danych;
	6. zmiany oprogramowania, aktualizacji oprogramowania oraz jego zabezpieczenia antywirusowego i sieciowego dokonuje Administrator Systemu Informatycznego.

**§ 23**

Ochrona zasobów danych osobowych przetwarzanych przez Spółdzielnię jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników i współpracowników Spółdzielni.

**ZAKRES ODPOWIEDZIALNOŚCI**

**§ 24**

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik i współpracownik Spółdzielni w zakresie zajmowanego stanowiska i posiadanych informacji.

**§ 25**

1. Inspektor Ochrony Danych w Spółdzielni:

1. informuje administratora oraz pracowników, którzy przetwarzają dane osobowe,
o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów o ochronie danych jak również doradza w tych sprawach;
2. monitoruje przestrzeganie rozporządzenia RODO oraz innych przepisów o ochronie danych jak również polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego
w operacjach przetwarzania oraz powiązane z tym audyty;
3. udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje ich wykonanie;
4. współpracuje z organem nadzorczym;
5. pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych
z przetwarzaniem oraz w stosownych przypadkach prowadzi konsultacje we wszelkich innych sprawach.

2. Inspektor Ochrony Danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

3. Spółdzielnia zapewni, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

4. Spółdzielnia będzie wspierała Inspektora Ochrony Danych w wypełnianiu przez niego zadań,
o których mowa w ust. 1 i zapewni mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

5. Spółdzielnia zapewni, by Inspektor Ochrony Danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Inspektor Ochrony Danych nie będzie odwoływany ani karany przez Spółdzielnię za wypełnianie swoich zadań. Inspektor Ochrony Danych bezpośrednio podlega Syndykowi.

6. Osoby, których dane dotyczą, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz
z wykonywaniem praw przysługujących im na mocy RODO.

7. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań - zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego.

8. Spółdzielnia zapewni, by inne zadania i obowiązki Inspektora Ochrony Danych nie powodowały konfliktu interesów ze sprawowaniem funkcji Inspektora Ochrony Danych Osobowych. W razie, gdyby taki konflikt wystąpił, priorytet będą miały zadania jako Inspektora Ochrony Danych Osobowych.

**§ 26**

1. Administrator Systemu Informatycznego odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;
2. optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego;
3. instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;
4. konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem;
5. nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;
7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego;
8. zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie;
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;
10. przyznawanie na wniosek Inspektora Ochrony Danych ściśle określonych praw dostępu do informacji w danym systemie;
11. wnioskowanie do Inspektora Ochrony Danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;
12. zarządzanie licencjami oraz procedurami ich dotyczącymi;
13. prowadzenie profilaktyki antywirusowej.

2. Praca Administratora Systemu Informatycznego jest nadzorowana przez Inspektora Ochrony Danych pod względem przestrzegania RODO oraz obowiązujących przepisów.

**PRZETWARZANIE DANYCH OSOBOWYCH**

**§ 27**

1. Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

2.Struktura zbiorów danych osobowych przetwarzanych w Spółdzielni jest określona
w **Załączniku nr 1** do Polityki Bezpieczeństwa.

**§ 28**

Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów informatycznych.

**§ 29**

Kopię bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

**ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE**

**§ 30**

Archiwizację dokumentów zawierających dane osobowe prowadzi się w odpowiednio zabezpieczonych pomieszczeniach i na właściwie zabezpieczonych nośnikach informatycznych lub tradycyjnych. Dane zbędne dla prowadzonych spraw są natychmiast niszczone przez działania fizyczne i informatyczne uniemożliwiające ich odczytanie.