1/1/03/2021

Uchwała nr... Zarządu Spółdzielni Mieszkaniowej „Agrodom" w Szczecinie
z dnia 8.03.2021r.
w sprawie przyjęcia Polityki ochrony danych w Spółdzielni Mieszkaniowej „Agrodom" w Szczecinie

Na podstawie art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w związku z art. 48 Prawa spółdzielczego z dnia 16 września 1982 r. tj. Dz.U. z 2017 r. poz. 1560 ze zmianami, uchwala się co następuje:

§ 1.

Wprowadza się w Spółdzielni Mieszkaniowej „Agrodom" w Szczecinie, zwanej dalej Spółdzielnią, Politykę ochrony danych w Spółdzielni Mieszkaniowej „Agrodom" w Szczecinie, stanowiącą **załącznik do niniejszej Uchwały**, zwaną Polityką.

§ 2.

1. Zobowiązuje się do zapoznania wszystkie osoby przetwarzające dane osobowe w Spółdzielni, z treścią dokumentu o którym mowa w § 1 i złożenia przez ww. osoby oświadczeń, których wzór zawiera **Załącznik nr 3 do Polityki**, w terminie do 30.04.2021 r.
2. Oświadczenia o których mowa w ust. 1 należy przekazać do Zarządu Spółdzielni.

§ 3.

Załącznik do uchwały stanowi dokument wewnętrzny stanowiący tajemnicę przedsiębiorstwa i nie podlega rozpowszechnianiu.

§ 4.

Uchwała wchodzi w życie z dniem podjęcia.

Dariusz Wociór
RADCA PRAWNY

41/10/2021

Załącznik do Uchwały nr... Zarządu Spółdzielni Mieszkaniowej „Agrodom" w Szczecinie z dnia 8.03.2021r.
w sprawie przyjęcia Polityki ochrony danych w Spółdzielni Mieszkaniowej „Agrodom" w Szczecinie

POLITYKA OCHRONY DANYCH W SPÓŁDZIELNI MIESZKANIOWEJ „AGRODOM" W SZCZECINIE

Rozdział 1 Postanowienia ogólne

§ 1.

Ilekroć w dokumencie jest mowa o:

1) **Polityka** - Politykę ochrony danych w Spółdzielni Mieszkaniowej „Agrodom" w Szczecinie

2) **RODO** – rozumie się przez to 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);

3) **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); 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;

4) **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

5) **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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;

6) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, **zwany także systemem IT**;

7) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

8) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

9) **administrator , zwanym także ADO**– rozumie się przez to **Spółdzielnię Mieszkaniową „Agrodom" w Szczecinie (zwaną dalej Spółdzielnią)** reprezentowaną przez Zarząd, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego;

10) **zgodzie osoby, której dane dotyczą** – oznacza 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;
11) **odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
12) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
13) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
14) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
15) **profilowaniu** – oznacza to dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
16) **pseudonimizacji** – oznacza to 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;
17) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;
18) **naruszeniu ochrony danych osobowych** – oznacza to 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;
19) **organ nadzorczy** – Prezes Urzędu Ochrony Danych.

§ 2.

1. Politykę stosuje się do wszystkich:
1) danych osobowych, w tym danych osobowych, wobec których Spółdzielnia jest Podmiotem Przetwarzającym,
2) osób przetwarzających dane osobowe w Spółdzielni,
3) osób posiadających dostęp do danych osobowych w Spółdzielni,
4) czynności przetwarzania danych osobowych,
5) kopii i nośników danych osobowych.
2. Polityka ochrony danych określa w szczególności:
1) prawa, obowiązki oraz granice dopuszczalnego zachowania osób przetwarzających dane osobowe w związku z działalnością Spółdzielni, Użytkowników systemów IT i tradycyjnych, w których przetwarzane są dane osobowe oraz konsekwencje naruszenia przepisów o ochronie danych osobowych,
2) sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę tych danych, w tym podstawowe warunki jakim powinny odpowiadać urządzenia z wykorzystaniem których dane są przetwarzane,

3) zasady prowadzenia dokumentacji związanej z przetwarzaniem danych osobowych,
4) wymagania w zakresie odnotowywania udostępniania danych osobowych,
5) zasady postępowania w sytuacji naruszenia ochrony danych osobowych,
3. Administrator przestrzega kodeksów postępowania zatwierdzonych i powszechnie obowiązujących zgodnie z przepisami, w celu zapewnienia odpowiednich zabezpieczeń danych. Administrator podejmuje wiążące i egzekwowalne zobowiązanie – w drodze umowy lub poprzez inne prawnie wiążące instrumenty – do stosowania tych odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.
4. Zastosowane zabezpieczenia mają zapewnić:
1) legalność – rozumianą jako przetwarzanie zgodnie z prawem,
2) poufność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom,
3) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
4) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
5) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej,
6) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
7) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, monitorowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji, które może dotyczyć systemów informatycznych i tradycyjnych służących do przetwarzania danych osobowych.
5. Wszystkie czynności podejmowane w celu realizacji niniejszej Polityki lub inne czynności podejmowane w zakresie dotyczącym przetwarzania lub ochrony danych osobowych w Spółdzielni muszą być należycie dokumentowane przez osoby te czynności podejmujące, tak, aby Spółdzielnia mogła wykazać przestrzeganie przepisów z zakresu ochrony danych osobowych, zgodnie z zasadą rozliczalności.

Rozdział 2 Organizacja systemu ochrony danych osobowych

§ 3.

1. Administratorem danych jest Spółdzielnia.
danych w zakresie stosowania przepisów o ochronie danych osobowych oraz wewnętrznych procedur działa Zarząd Spółdzielni. Obowiązki określone w Polityce wypełnia w imieniu Administratora Zarząd chyba, że wskazano inną osobę.

3. Zarząd Spółdzielni w szczególności:
1) Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
4. Po przeprowadzeniu analizy nie wyznacza Inspektora Ochrony Danych (IOD)
5. Do kompetencji Zarządu Spółdzielni należy w szczególności:
1) zapewnianie zapoznania i informowanie Rady Nadzorczej oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych i doradzanie im w tej sprawie;

2) monitorowanie przestrzegania RODO i innych przepisów o ochronie danych oraz niniejszej Polityki, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego.
6) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
7) nadzorowanie przestrzegania zasad ochrony danych osobowych tj. środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, ze szczególnym uwzględnieniem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w tym nadzór nad obiegiem oraz przechowywaniem materiałów i dokumentów zawierających dane osobowe,
8) nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych, środki ich ochrony oraz przestrzegania zasad w niej określonych,
9) nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych oraz pozostałych wniosków dotyczących bezpieczeństwa informacji, w tym danych osobowych, a także nadzór w zakresie realizacji tych wniosków,
10) nadzór nad fizycznym zabezpieczeniem pomieszczeń w których przetwarzane są dane osobowe oraz organizacją kontroli przebywających w nich osób,
11) zapewnienie przeciwdziałania naruszeniom oraz prowadzenie rejestru naruszeń,
6. Do zadań Zarządu Spółdzielni należy zapewnienie działania infrastruktury teleinformatycznej i oprogramowania w sposób zapewniający właściwy poziom bezpieczeństwa informacji wynikający z obowiązujących przepisów i procedur wewnętrznych;
7. Nadzorowanie przez Zarząd przestrzegania bezpieczeństwa danych osobowych gromadzonych i przetwarzanych w systemach IT ma na celu zabezpieczenie ich przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
8. Do kompetencji Zarządu należy w szczególności:
1) zapewnienie właściwego poziomu bezpieczeństwa systemu informatycznego, w tym danych osobowych w nich przetwarzanych,
2) zapewnienie mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych,
3) inicjatywa w zakresie zapewnienia alternatywnego, awaryjnego zasilania systemu informatycznego oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych, w tym analizowanie stanu zabezpieczeń w zakresie centralnego awaryjnego zasilania budynku,
4) podejmowanie działań zabezpieczających system informatyczny w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu, informacji o zmianach w sposobie działania systemu lub innych urządzeń wskazującej na naruszenie bezpieczeństwa danych,
5) zapewnienie ochrony systemu teleinformatycznego oraz danych osobowych przesyłanych za pośrednictwem tych systemów,
6) zapewnienie ochrony danych osobowych w związku z naprawą, konserwacją oraz likwidacją systemu informatycznego, w tym urządzeń komputerowych, na których zapisane są dane osobowe,

7) wnioskowanie i opiniowanie wniosków do Zarządu Spółdzielni o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych w systemie IT oraz realizacja tych czynności po akceptacji przez Zarząd Spółdzielni,
8) zapewnienie przeglądów, konserwacji oraz uaktualnień systemu służącego do przetwarzania danych osobowych, w tym w szczególności z uwzględnieniem specyfiki działalności Spółdzielni,
9) przestrzeganie przepisów bhp i ppoż. w przynależnych pomieszczeniach.
9. Zarząd Spółdzielni wspólnie z pracownikami oraz osobami współpracującymi na poszczególnych stanowiskach pracy co najmniej raz w roku przeprowadza kompleksowy audyt wewnętrzny ochrony danych osobowych w Spółdzielni.
10. Zarząd Spółdzielni wspólnie z pracownikami oraz osobami współpracującymi na poszczególnych stanowiskach pracy przeprowadza pozaplanowy audyt wewnętrzny ochrony danych osobowych w Spółdzielni przypadku:
- stwierdzenia naruszenia lub jego prawdopodobieństwa,
- zmian w procesie przetwarzania danych osobowych,
- zmiany standardów przetwarzania danych osobowych,
- wydania wytycznych dotyczących obszaru przetwarzania danych osobowych istniejącego u administratora,
- skargi osoby, której dane dotyczą na niezgodne z prawem przetwarzanie danych osobowych;
- podjęcia decyzji przez Zarząd Spółdzielni.
11. Z przeprowadzonych audytów spisuje się raporty, które są podstawą zmian w systemie ochrony danych osobowych.

Rozdział 3 Przetwarzanie danych osobowych i procedury odbierania zgód

§ 4.

1. Wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne.
2. Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem.
3. W szczególności konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.
4. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami.
5. Należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe.
6. Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do

nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

7. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- 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;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora 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.

8. Zgoda może być podstawa prawną przetwarzania danych osobowych w Spółdzielni wówczas, jeżeli Spółdzielnia:

1) nie może oprzeć przetwarzania danych osobowych na innej podstawie prawnej,
2) jest w stanie zapewnić, że spełni wszystkie warunki uzyskania ważnej zgody,
3) jest w stanie zrealizować prawo do cofnięcia zgody.

9. Zgoda osoby, której Dane Osobowe dotyczą, musi być:

1) dobrowolna, to znaczy, że osoba wyrażająca zgodę posiada realną możliwość wyboru w odniesieniu do przyjęcia lub odrzucenia zaoferowanych warunków lub odrzucenia ich bez niekorzystnych konsekwencji oraz ma możliwość sprawowania kontroli nad swoimi danymi. Zgoda nie będzie dobrowolna, jeżeli pojawi się jakikolwiek element przymusu, presji lub braku możliwości swobodnego złożenia oświadczenia woli lub jeżeli nie będzie szczegółowa, tj. jeżeli nie będzie umożliwiała wyboru pomiędzy wyrażeniem zgody na różne, oddzielne czynności przetwarzania. Wyrażenie zgody nie może stanowić niepodlegającej negocjacji części warunków, a odmowa jej wyrażenia nie może stanowić podstawy odmowy zrealizowania przez tę osobę swojego celu; wyrażenie zgody może być warunkiem koniecznym do zawarcia umowy ze Spółdzielnią lub do skorzystania z określonego świadczenia tylko wtedy, gdy zgoda stanowi jedyną możliwą przesłankę przetwarzania tych danych osobowych, a więc Spółdzielnia musi posiadać tę zgodę, jeżeli chce być zgodny z RODO oraz jeżeli zakres zgody dotyczy wyłącznie danych osobowych i czynności przetwarzania niezbędnych do realizacji określonego przetwarzania.
2) świadoma, to znaczy, że osoba wyrażająca zgodę wie, na co się godzi i posiada pełną informację dotyczącą okoliczności planowanego przetwarzania danych osobowych pozwalającą jej na podjęcie świadomej decyzji, w szczególności zna cele przetwarzania oraz zakres przetwarzanych danych osobowych;
3) konkretna, to znaczy, że musi obejmować konkretne cele i operacje przetwarzania danych osobowych, szczegółowo określać cele przetwarzania jako zabezpieczenie przed zmianą celu w trakcie tego przetwarzania oraz być wyraźnie oddzielona od informacji na inne tematy;
4) jednoznaczna, to znaczy, że zgoda zawsze musi być wyrażona poprzez aktywne działanie lub oświadczenie; nie może stanowić nieodznaczenia wcześniej już zaznaczonych pól; nie może zostać wyrażona przez milczenie, bezczynność lub dalsze korzystanie z usługi; nie może stanowić tej samej czynności co zawarcie umowy lub zaakceptowanie ogólnych warunków

usługi.

10. Osoba, której dane osobowe dotyczą, jest informowana przed wyrażeniem zgody o prawie do jej cofnięcia w każdej chwili i bez podawania przyczyny, lecz bez wpływu na zgodność z prawem przetwarzania danych osobowych przed cofnięciem, co oznacza, że cofnięcie zgody nie spowoduje niezgodności z prawem przetwarzania dokonanego przed cofnięciem zgody.

11. Zgoda może zostać wyrażona:

1) przez złożenie oświadczenia woli o wyrażeniu zgody (zgoda wyraźna) – np. poprzez podpisanie klauzuli zgody, zaznaczenie osobnego check-boxu, zaznaczenie odpowiedniego miejsca krzyżykiem, skreślenie niewłaściwego oświadczenia,

2) przez dokonanie wyraźnego działania potwierdzającego wyrażenie zgody, czyli przez świadome podjęcie celowego działania, aby wyrazić zgodę na określone przetwarzanie – np. poprzez przesłanie dokumentu do Spółdzielni.

12. Zgoda wyrażona poprzez wyraźne działanie potwierdzające nie może być podstawą przetwarzania danych osobowych szczególnych kategorii.

13. Aby zgoda wyrażana poprzez wyraźne działanie potwierdzające była ważna, osoba, której dane osobowe dotyczą, musi być świadoma, że dokonując określonej czynności potwierdza, że chce, aby Spółdzielnia przetwarzała jej dane osobowe w konkretnym celu. Z tego powodu, jeżeli Spółdzielnia z własnej inicjatywy pozyskuje dane osobowe, które będzie przetwarzał na podstawie zgody wyrażonej poprzez wyraźne działanie potwierdzające, informuje o tym osobę, której dane osobowe dotyczą, przed dokonaniem przez nią tego działania potwierdzającego.

14. Klauzula zgody zawiera:

1) nazwę Spółdzielni,

2) cele przetwarzania danych osobowych,

3) określenie czynności przetwarzania, które objęte są wyrażoną zgodą,

4) informację o prawie do cofnięcia zgody w każdej chwili i bez podawania powodu, lecz bez wpływu na zgodność z prawem przetwarzania Danych Osobowych przed cofnięciem,

5) skutki niewyrażenia lub późniejszego cofnięcia zgody,

6) informację, czy wyrażenie zgody jest obowiązkowe do skorzystania z określonej usługi,

7) oświadczenie woli o wyrażeniu zgody, a jeżeli zgoda jest wyrażana poprzez wyraźne działanie potwierdzające – informację o tym, jakie działanie spowoduje skutek w postaci wyrażenia zgody,

8) wskazanie, gdzie można znaleźć pełną klauzulę informacyjną.

15. Przetwarzanie danych osobowych na podstawie zgody osoby nie zwalnia Spółdzielni od obowiązku przestrzegania podstawowych zasad przetwarzania danych osobowych, w szczególności zasady ograniczenia celu oraz minimalizacji.

16. Każda osoba, której dane osobowe dotyczą, ma prawo do cofnięcia wyrażonej zgody.

17. Spółdzielnia zapewnia, aby cofnięcie zgody:

1) było tak samo łatwe, jak jej wyrażenie,

2) może odbywać się w inny sposób, niż jej wyrażenie,

3) nie powodowało negatywnych konsekwencji dla osoby, której dane osobowe dotyczą, w szczególności, aby było bezpłatne i nie pociągało za sobą obniżenia poziomu usługi.

18. Jeżeli osoba, której dane osobowe dotyczą, skutecznie cofnęła zgodę, Spółdzielnia niezwłocznie zaprzestaje przetwarzania Danych Osobowych w celach, dla których zgodę pozyskiwał, a jeżeli nie ma innej ważnej podstawy prawnej do przetwarzania Danych Osobowych, usuwa te Dane Osobowe.

19. Ocena prawnie uzasadnionego interesu jest prowadzona w wyniku testu równowagi wykonywanego przez Zarząd Spółdzielni. Test równowagi jest wykonywany również w innych uzasadnionych przypadkach.

20. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:
- przetwarzane zgodnie z prawem;
- zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
- merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

21. Zakazane jest przetwarzanie danych osobowych:
1) na zapas,
2) bez określonego celu, wyłącznie dla samego posiadania danych osobowych bez sprecyzowanej potrzeby,
3) przez okres dłuższy niż dane osobowe są potrzebne.

22. Każda zmiana w obszarze przetwarzania danych osobowych, w szczególności rozpoczęcie przetwarzania nowych kategorii danych osobowych, rozszerzenie lub zmiana zakresu obecnie przetwarzanych danych osobowych, zmiana celów przetwarzania lub okoliczności związanych z przetwarzaniem danych osobowych wymaga uprzedniej akceptacji Zarządu Spółdzielni.

23. Upoważniony pracownik o planowanej zmianie związanej ze zmianą w obszarze przetwarzania danych osobowych w Spółdzielni jest obowiązana zgłosić ten fakt Zarządowi Spółdzielni niezwłocznie po rozpoczęciu działań mających na celu wprowadzenie planowanej zmiany.

24. Po otrzymaniu informacji o planowanej zmianie, Zarząd Spółdzielni dokonuje weryfikacji planowanych czynności przetwarzania pod względem RODO, tj.:
1) weryfikacji zgodności planowanego przetwarzania z ogólnymi zasadami przetwarzania danych osobowych,
2) weryfikacji podstawy prawnej do planowanego przetwarzania danych osobowych, zgodnie z art. 6, 9 i 10 RODO,
3) jeżeli przetwarzanie danych osobowych będzie odbywało się na podstawie zgody, weryfikacji poprawności treści klauzuli zgody oraz planowanego sposobu jej pozyskiwania,
4) weryfikacji poprawności planowanej treści i sposobu spełniania obowiązków informacyjnych wobec osób, których dane osobowe dotyczą,
5) weryfikacji planowanych zabezpieczeń danych osobowych, w tym przestrzegania obowiązku uwzględniania ochrony danych osobowych w fazie projektowania oraz domyślnej ochrony Danych Osobowych,
6) weryfikacji konieczności przeprowadzenia oceny skutków dla ochrony danych, a w przypadku wystąpienia takiej konieczności zgodnie z RODO – koordynacji jej przeprowadzenia i sporządzenia odpowiedniego raportu,
7) jeżeli z planowanym przetwarzaniem danych osobowych wiąże się powierzenie przetwarzania – weryfikacji poprawności planowanej treści umowy powierzenia przetwarzania danych osobowych,
8) jeżeli planowane jest powierzenie przetwarzania przez Spółdzielnię do innego podmiotu, weryfikacji zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane osobowe dotyczą, przez planowanego przetwarzającego,
9) jeżeli z planowanym przetwarzaniem wiąże się transfer danych osobowych poza granice Polski – weryfikacji, czy dochodzi do transferu Danych Osobowych do państwa trzeciego oraz podstaw prawnych do dokonywania planowanego transferu.

25. Po dokonaniu weryfikacji Zarząd Spółdzielni wydaje akceptację, odpowiednie rekomendacje albo odmawia akceptacji.

26. Przetwarzanie danych osobowych stanowiących tajemnicę prawnie chronioną, np. tajemnicę zawodową jest objęte dodatkowymi wymogami wynikającymi z przepisów regulujących tę tajemnicę.

§ 5.

Przetwarzanie danych osobowych odbywa się z wykorzystaniem dokumentów, materiałów, przesyłek analogowych (nieelektronicznych), wniosków, pism, akt osobowych pracowników, dokumentów finansowo-księgowych, podań itp. oraz danych zawartych na nośnikach elektronicznych, magnetycznych, optycznych i elektronicznych, w tym przekazywanych drogą elektroniczną, jako załączniki do przesyłek analogowych, a także danych przetwarzanych w systemie kadrowo-płacowym, systemie do obsługi dokumentów ubezpieczeniowych i wymianie informacji z ZUS, Urzędem Skarbowym, systemie teleinformatycznym Spółdzielni.

§ 6.

1. Obszarem przetwarzania danych osobowych są wydzielone pomieszczenia lub części pomieszczeń w siedzibie **Spółdzielni Mieszkaniowej „Agrodom" w Szczecinie** znajdującej się przy **ul. Ks. Niemcewicza 16b/10 w Szczecinie (załącznik nr 1 do Polityki).**
2. Nadzór nad dostępem do pomieszczeń, w których przetwarzane są dane osobowe sprawuje **Zarząd Spółdzielni.**
3. Pracownicy i inne osoby przebywające w obszarze przetwarzania są zobowiązani do informowania Zarzadu o zauważonych próbach nieuprawnionego dostępu do pomieszczeń, o których mowa w ust. 1.
4. Po godzinach urzędowania dostęp do pomieszczeń mają upoważnieni pracownicy oraz osoby upoważnione pisemnie przez Zarząd Spółdzielni.
5. Zarząd Spółdzielni może określić pomieszczenia, do których dostęp osób sprzątających i innych będzie ograniczony i możliwy tylko pod nadzorem osób uprawnionych do przebywania w tych pomieszczeniach np. archiwa, serwerownie. Na drzwiach takich pomieszczeń umieszcza się informację: *Pomieszczenie służbowe, nieupoważnionym wstęp wzbroniony.*
6. Na drzwiach pomieszczeń w których obsługiwani są interesanci umieszcza się informację: *Interesanci obsługiwani są pojedynczo.*
7. Osoby opuszczające pomieszczenie za które są odpowiedzialne, w którym nikt nie przebywa i przetwarzane są dane osobowe, zobowiązane są do zamknięcia drzwi na klucz. Zabrania się pozostawiania klucza w drzwiach po ich zewnętrznej stronie, za wyjątkiem sytuacji związanych z ochroną przeciwpożarową.
8. Zabrania się samowolnego dorabiania kluczy oraz ich wynoszenia poza siedzibę Spółdzielni. Każdorazowa potrzeba dorobienia dodatkowego klucza lub kluczy winna być zgłoszona Zarządowi Spółdzielni, który wyraża na to pisemną zgodę oraz określa zasady wykonania oraz posługiwania się kopią klucza/kluczy.
9. Po zakończeniu pracy pracownik zobowiązany jest wylogować się z systemu informatycznego, zamknąć okna w pomieszczeniu, umieścić materiały i dokumenty zawierające dane osobowe w szafach lub szufladach zamykanych na klucz, zgodnie z zasadą czystego biurka, czystej drukarki i czystej kopiarki (o ile takie urządzenia znajdują się w pomieszczeniu) zniszczyć w niszczarce wszystkie materiały przeznaczone do zniszczenia w postaci błędnie utworzonej lub niepotrzebnej dokumentacji mającej krótkotrwałe znaczenie praktyczne, m.in. wydruków komputerowych i innych materiałów analogowych zawierających dane osobowe lub umieścić w miejscu oznaczonym: *Dokumenty do zniszczenia.*

§ 7.

1. Wszystkie osoby, które posiadają dostęp do danych osobowych w obszarze wymienionym w § 6 muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Zarząd Spółdzielni oraz podpisać oświadczenie o zachowaniu poufności.
2. Zarząd Spółdzielni dokonuje weryfikacji upoważnień raz w roku i dokonuje ewentualnych zmian.
3. Wzór upoważnienia dla pracowników oraz osób współpracujących ze Spółdzielnią na podstawie umów cywilnoprawnych, stanowi **załącznik nr 2 do Polityki.**
4. Wzór oświadczenia o zachowaniu poufności dla pracowników oraz osób współpracujących ze Spółdzielnią na podstawie umów cywilnoprawnych, stanowi **załącznik nr 3 do Polityki.**
5. Wzór upoważnienia dla osób będących członkami Rady Nadzorczej i członkami innych organów samorządowych w Spółdzielni, stanowi **załącznik nr 4 do Polityki**.
6. Wzór oświadczenia o zachowaniu poufności dla osób będących członkami Rady Nadzorczej w Spółdzielni, stanowi **załącznik nr 5 do Polityki**.
7. Zakres upoważnień określonych w powyższych ustępach został określony na podstawie łączącej upoważnionego ze Spółdzielnią umowy.
8. Warunkami koniecznymi przetwarzania danych osobowych przez upoważnionych jest łączne spełnienie przesłanek:
1) nadanie przez Zarząd upoważnienia i potwierdzenie odbioru upoważnienia przez osobę upoważnioną;
2) podpisanie przez pracownika Spółdzielni, członka Rady Nadzorczej oświadczenia o poufności o którym mowa w ust. 3 lub 5;
3) wprowadzenie danych osoby upoważnionej do ewidencji o której mowa w ust. 10;
4) zapoznanie się przez pracownika Spółdzielni, członka Rady Nadzorczej, Rady ... z przepisami dotyczącymi ochrony danych osobowych i procedur obowiązujących w Spółdzielni poprzez odbycie szkolenia prowadzonego przez osobę upoważnioną przez Zarząd Spółdzielni.
9. Uprawnienia do systemów informatycznych służących do przetwarzania danych osobowych nadawane są wyłącznie osobom upoważnionym do przetwarzania określonych danych osobowych.
10. Uprawnienia do systemów informatycznych są nadawane przez Zarząd Spółdzielni.
11. Uprawnienia do systemów informatycznych nadawane są w zakresie najwęższym, lecz umożliwiającym swobodną realizację zadań przez użytkownika.
12. Każda osoba przetwarzająca dane osobowe w systemie informatycznym otrzymuje nazwę użytkownika (login). Raz użyty login nie może być używany ponownie, nawet jeśli użytkownik zakończył już pracę w Spółdzielni.
13. Użytkownicy systemu informatycznego przetwarzającego Dane Osobowe wykorzystują w procesie uwierzytelnienia identyfikatory (loginy) i hasła.
14. Hasło jest nadawane samodzielnie przez użytkownika systemu.
15. Hasło do systemu służącego do przetwarzania danych osobowych:
1) musi składać się co najmniej z 10 znaków, w tym zawierać co najmniej małą i dużą literę, cyfrę lub znak specjalny,
2) nie może składać się ze słów, cyfr, liczb lub ich kombinacji łatwych do odgadnięcia, w szczególności: nazwy miesiąca, oznaczenia roku, daty urodzenia, imienin swoich lub osób bliskich, imion, nazwisk lub pseudonimów swoich lub osób bliskich, tytułów filmów, utworów muzycznych, książek, słów związanych z zainteresowaniami, pasjami, hobby.
15. Hasło należy zmieniać co najmniej raz na 30 dni, niezależnie od tego, czy system informatyczny wymusza jego zmianę.
16. W przypadku, gdy doszło do kompromitacji (odgadnięcia, ujawnienia, podglądnięcia itd.) hasła użytkownika lub użytkownik podejrzewa, że mogło do niej dość, tj. że jego hasło jest znane innej osobie, jest obowiązany niezwłocznie zmienić hasło oraz poinformować o tym fakcie Zarząd Spółdzielni.

17. Użytkownik zobowiązany jest do:
1) niezapisywania haseł, w szczególności ich nieumieszczania w miejscach dostępnych dla osób trzecich,
2) nieujawniania hasła innym osobom,
3) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
4) przestrzegania zasad dotyczących zmian hasła,
5) wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez osoby trzecie.
18. Proces uwierzytelniania składa się z wprowadzenia nazwy użytkownika oraz poufnego hasła.
19. Każdy użytkownik jest obowiązany wykonywać pracę z użyciem własnych danych uwierzytelniających: nazwy użytkownika oraz hasła. Jeżeli tę samą pracę powinna wykonać lub kontynuować inna osoba, należy wystąpić do Zarzadu o nadanie kolejnej osobie uprawnień podobnych lub tożsamych.
20. Zakazane jest udostępnianie danych uwierzytelniających innej osobie, w tym przełożonym lub osobom przeprowadzającym kontrole, audyty, inspekcje.
21. Przy wprowadzaniu danych uwierzytelniających użytkownik jest obowiązany upewnić się, że wprowadzone hasło nie będzie widoczne dla żadnej innej osoby, a ekran monitora nie jest w zasięgu monitoringu wizyjnego.

22. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do ochrony danych osobowych przed dostępem do nich osób nieuprawnionych, niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

23. Osoby upoważnione zobowiązane są do zabezpieczenia materiałów zawierających dane osobowe w sposób uniemożliwiający nieuprawniony dostęp do danych osobowych osobom nieupoważnionym do ich przetwarzania, nieuprawnione ujawnienie danych osobowych, nieautoryzowany dostęp, niedozwolone: powielenie, modyfikację, zniszczenie, utratę, nieprawidłowe wykorzystanie lub kradzież.

24. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej osoby upoważnione zobowiązane są do niepozostawiania materiałów zawierających dane osobowe w miejscach umożliwiających fizyczny dostęp do nich osobom nieuprawnionym. Po zakończeniu pracy lub podczas czasowej przerwy w pracy, jeżeli dostęp do pomieszczenia mają osoby nieposiadające upoważnienia, materiały zawierające dane osobowe powinny być przechowywane w szafach lub szufladach zamykanych na klucz (tzw. zasada czystego biurka). Niedopuszczalne jest pozostawianie materiałów zawierających dane osobowe na biurku, regale, w niezamkniętej szafie i innych miejscach, do których mają dostęp inne osoby.

25. Jeżeli dostęp do zamkniętego pomieszczenia posiadają wyłącznie osoby upoważnione do przetwarzania danych osobowych tam przechowywanych, a poza godzinami pracy nikt inny nie ma dostępu do tego pomieszczenia, w tym serwis sprzątający i ochrona fizyczna, można odstąpić od przestrzegania zasady czystego biurka.

26. Kopiowanie danych osobowych może odbywać się wyłącznie przez osobę upoważnioną w ramach posiadanego przez nią upoważnienia do przetwarzania danych osobowych, w związku z realizacją czynności zawodowych w Spółdzielni. Kopie danych osobowych podlegają zniszczeniu niezwłocznie po realizacji celu, dla którego zostały wykonane.

27. Dokonywanie wydruków, skanowanie lub kopiowanie materiałów zawierających dane osobowe odbywa się wyłącznie przy obecności osoby upoważnionej przy urządzeniu. Niedozwolone jest pozostawianie urządzenia w trakcie drukowania/skanowania/kopiowania bez nadzoru, jeżeli materiały znajdujące się w urządzeniu zawierają dane osobowe.

28. Każdy dokument papierowy zawierający dane osobowe sporządzony jako dokument roboczy należy najpóźniej na koniec dnia pracy zniszczyć lub zamknąć w miejscu uniemożliwiającym dostęp osób nieuprawnionych.

29. Niszczenia brudnopisów, błędnych lub zbędnych kopii materiałów żawierających dane osobowe dokonuje się wyłącznie w dedykowanych niszczarkach lub umieszcza w dedykowanych kontenerach na dokumenty przeznaczone do zniszczenia przez podmiot profesjonalny.

30. Osoby upoważnione do przetwarzania danych osobowych nie mogą ich ujawniać zarówno w Spółdzielni, jak i poza nią, w zakresie wykraczającym poza wykonywanie swoich obowiązków.

31. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza teren Spółdzielni bez związku z wykonywaniem czynności zawodowych.

32. Zarząd Spółdzielni prowadzi, w tym aktualizuje, rejestr czynności przetwarzania danych osobowych zgodnie z art. 30 ust. 1 RODO. Wzór rejestru czynności przetwarzania danych osobowych stanowi **załącznik nr 6 do Polityki.**

33. Zarząd Spółdzielni prowadzi, w tym aktualizuje, rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora zgodnie z art. 30 ust. 2 RODO. Wzór rejestru wszystkich kategorii czynności przetwarzania stanowi **załącznik nr 7 do Polityki.**

34. Ewidencja osób upoważnionych jest prowadzona zgodnie z wzorem stanowiącym **załącznik nr 8 do Polityki**.

35. Każdy pracownik w zakresie czynności wykonywanych na stanowisku pracy zgłasza do wprowadzenia w dzienniku korespondencyjnym każdy wniosek o udostępnienie danych osobowych oraz odpowiedź na wniosek. Pracownik lub dział w Spółdzielni za pisemną zgodą Zarządu może prowadzić dziennik korespondencyjny w którym ewidencjonuje wszelkie udostępnienia danych osobowych. Nie dotyczy to udostępniania danych z systemu informatycznego jeżeli w systemie jest prowadzony „automatyczny" wykaz udostępnień.

36. Osobom przebywającym w obszarze przetwarzania danych osobowych, które nie przetwarzają danych osobowych udzielana jest Zgoda na przebywania w obszarze przetwarzania danych , której wzór stanowi **załącznik nr 9 do Polityki.**

37. Za przestrzeganie przepisów z zakresu ochrony danych osobowych w Spółdzielni odpowiada każdy pracownik w zakresie:
1) przestrzegania zasad bezpieczeństwa danych osobowych,
2) przestrzegania Polityki, procedur i instrukcji,
3) zgłaszania Zarządowi Spółdzielni wszystkich okoliczności związanych z przetwarzaniem danych osobowych, w szczególności w przypadkach wskazanych w Polityce,
4) przestrzegania zaleceń i rekomendacji Zarządu w zakresie dotyczącym Danych Osobowych.

38. Naruszenie Polityki, procedur lub instrukcji lub odmowa realizacji zaleceń lub rekomendacji Zarządu Spółdzielni z jednoczesnym niezawiadomieniem o tym odpowiedniej osoby zgodnie z niniejszą Polityką stanowi naruszenie podstawowych obowiązków pracownika w rozumieniu ustawy z 26.6.1974 r. – Kodeks pracy (t.j. Dz.U. z 2018 r. poz. 917 ze zm.), w tym może stanowić ciężkie naruszenie tych obowiązków i być przedmiotem postępowania dyscyplinarnego, w tym zwolnienia z winy pracownika bez okresu wypowiedzenia, zgodnie z Kodeksem pracy.

39. Naruszenie zasad niniejszej Polityki może skutkować wyciągnięciem konsekwencji wobec osób zatrudnionych na umowy cywilnoprawne oraz osób związanych ze Spółdzielnią inną umową – zgodnie z treścią tych umów oraz przepisów ogólnych, w szczególności Kodeksu cywilnego.

40. Członkowie Rady Nadzorczej ponoszą odpowiedzialność za zawinioną szkodę wyrządzoną Spółdzielni w zakresie ochrony danych osobowych.

§ 8.

Uprawnienia do przetwarzania danych osobowych w systemach informatycznych nadawane są zgodnie z procedurą określoną w § 7. Uprawnienia, o których mowa w zdaniu pierwszym, ważne są do dnia odwołania lub do chwili ustania zatrudnienia uprawnionego pracownika.

§ 9.

1. Wszyscy pracownicy posiadający dostęp do danych osobowych przed przystąpieniem do pracy uczestniczą w szkoleniach dotyczących obowiązujących przepisów prawa z zakresu ochrony danych osobowych oraz obowiązujących w Spółdzielni procedur wewnętrznych;
2. Zakres czynności dla osoby upoważnionej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę przetwarzanych danych osobowych w stopniu adekwatnym do jej zadań na stanowisku pracy.

§ 10.

1. Udostępnianie drogą pocztową lub kurierską dokumentów i materiałów zawierających dane osobowe może odbywać się listem zwykłym, a w przypadku danych zawartych na nośnikach magnetycznych, optycznych lub elektronicznych – przesyłką rejestrowaną.
2. Pracownicy Spółdzielni przygotowujący przesyłki, o których mowa w ust. 1 powinni dołożyć należytej staranności celem zabezpieczenia ich zawartości przed nieuprawnionym dostępem do ich zawartości osób trzecich;
3. W Spółdzielni dopuszcza się stosowanie dodatkowych zabezpieczeń technicznych i organizacyjnych.

§ 11.

1. Użytkownik zobowiązany jest do dbania o bezpieczeństwo poczty elektronicznej, w szczególności do używania silnego hasła dostępu, nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł oraz zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od nieznanych nadawców;
2. Szczegółowe procedury korzystania z poczty elektronicznej oraz konfiguracji sprzętu komputerowego Użytkownika systemu informatycznego reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Spółdzielni.

3. Kopiowanie danych osobowych na przenośne nośniki informacji danych jest zabronione, chyba że spełnione są łącznie następujące warunki:

1) ich sporządzenie jest niezbędne do realizacji obowiązków służbowych,
2) nośnik jest nośnikiem służbowym Spółdzielni,
3) Zarząd Spółdzielni wyraził zgodę na przetwarzanie tych Danych Osobowych na przenośnym nośniku informacji.
4. Służbowe mobilne nośniki danych osobowych są zabezpieczone za pomocą narzędzi szyfrujących zatwierdzonych przez Spółdzielnię.
5. Zarząd Spółdzielni prowadzi wykaz służbowych mobilnych nośników Danych Osobowych zatwierdzonych w Spółdzielni.

Rozdział 4. Procedura retencji danych osobowych

§ 12

W przypadku gdy dla określonych danych osobowych nie występują żadne prawnie uzasadnione cele przetwarzania ADO zaprzestaje realizowania jakichkolwiek operacji na tych danych osobowych, z wyjątkiem ich usunięcia lub nieodwracalnej anonimizacji (przez którą rozumie się modyfikację danych osobowych w taki sposób, że nie jest możliwa identyfikacja podmiotów danych).

§ 13

1. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, Zarząd Spółdzielni powinien ustalić termin ich usuwania i przeprowadzić okresowy, co najmniej raz w roku przegląd.
2. W przypadku gdy okres retencji danych osobowych nie wynika wyraźnie z przepisów prawa, Zarząd Spółdzielni ustala te okresy samodzielnie, uwzględniając ogólne zasady przetwarzania danych osobowych przewidziane w RODO i określa w rejestrze czynności przetwarzania. W przypadku gdy okres retencji wynika z przepisów prawa, ma on pierwszeństwo.
3. Dane osobowe mogą być przetwarzane dłużej niż wynosi okres retencji w przypadku gdy są one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, pod warunkiem, że wdrożone są odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności podmiotów danych.
4. Okres retencji danych osobowych Zarząd Spółdzielni określa w rejestrze czynności przetwarzania.
5. Okresy retencji określone w rejestrze czynności przetwarzania mogą ulegać zmianie w przypadku zmiany przepisów prawnych lub decyzji Zarządu Spółdzielni.
6. Zarząd Spółdzielni określa w uchwałach zasady i terminy usuwania danych osobowych.
7. Przed usunięciem danych osobowych należy zweryfikować, czy nie zachodzą przesłanki wydłużenia okresu retencji, w szczególności poprzez sprawdzenie, czy:
- nie występuje obowiązek prawny ciążący na Spółdzielni, który nie został uwzględniony w rejestrze czynności przetwarzania;
- nie nastąpiło przerwanie lub zawieszenie okresu przedawnienia roszczeń, zgodnie z właściwymi przepisami, skutkujące koniecznością dalszego przetwarzania danych osobowych;
- dalsze przechowywanie nie jest konieczne w związku z biegnącym okresem przedawnienia zobowiązań podatkowych.
8. Usunięcie danych osobowych powinno nastąpić niezwłocznie po upływie okresu retencji, z uwzględnieniem okresu koniecznego do podjęcia niezbędnych czynności technicznych i organizacyjnych związanych z usunięciem danych osobowych.

Rozdział 5. Monitoring wizyjny

§ 14.

1. Teren Spółdzielni może być monitorowany urządzeniami nagrywającymi obraz.
2. Celem zamontowania kamer w Spółdzielni nagrywających obraz jest ochrona bezpieczeństwa i mienia Spółdzielni oraz jej członków i osób nie będących członkami, którym przysługują prawa do lokali.
3. Decyzję o zamontowaniu kamer podejmuje Zarząd Spółdzielni.
4. Zarząd odpowiada za zabezpieczenie, funkcjonowanie monitoringu oraz przechowywanie i udostępnianie nagrań monitoringu oraz niszczenie (usuwanie) nagrań.
5. Teren objęty zakresem monitoringu powinien być oznaczony tabliczkami informującymi, że Spółdzielnia monitoruje teren i nagrywa obraz. Na tablicach informacyjnych powinny być umieszczone informacje określające: nazwę, adres, dane kontaktowe Spółdzielni jako administratora, określenie Teren / budynek monitorowany i wskazanie gdzie znajduje się

klauzula informacyjna w zakresie przetwarzania danych w monitoringu wizyjnym.
6. Klauzulę informacyjną dotyczącą monitoringu wizyjnego umieszcza się na tablicy informacyjnej w siedzibie Spółdzielni oraz na stronie internetowej Spółdzielni w zakładce RODO.
7. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring) zgodnie z Kodeksem pracy.

§ 15

1. Zarząd Spółdzielni odpowiada za właściwe przechowywanie i zabezpieczenie zapisu przed dostępem do niego osób nieuprawnionych.
2. Do monitoringu powinni mieć dostęp tylko członkowie Zarządu oraz pisemnie upoważnieni pracownicy.
3. Po upływie terminu przechowywania zapis usuwa się z nośników samoczynnie w sposób uniemożliwiający jego odzyskanie. Jeżeli nośników nie można wykorzystać ponownie, należy je zniszczyć.

§ 16

1. Dane pochodzące z nagrań kamer monitoringu wizyjnego umożliwiające identyfikację osoby oraz nagrywanie jej głosu, zarejestrowane i przechowywane uważane są za dane osobowe.
2. Administratorem danych jest Spółdzielnia, która jest zobowiązana wykonywać obowiązki wynikające z przepisów o ochronie danych osobowych.
3. Zarząd Spółdzielni udostępnia zapis na pisemny wniosek uprawnionego podmiotu.
4. Podmiotami uprawnionymi do wglądu w zapis monitoringu są organy ścigania, sądy, instytucje państwowe i samorządowe oraz inne podmioty, w tym osoby fizyczne, po wskazaniu podstaw prawnych, faktycznych i interesu prawnego

Rozdział 6. Obsługa interesantów, doręczanie korespondencji, udostępnianie informacji

§ 17

1. Przed udzieleniem informacji bezpośredniej tożsamość interesantów powinna być zweryfikowana poprzez żądanie okazania dokumentu tożsamości celem sprawdzenia uprawnień dostępu do danych osobowych oraz weryfikację podstaw prawnych i faktycznych udzielenia informacji.
2. Interesanci powinni być obsługiwani pojedynczo.
3. Pracownicy Spółdzielni zobowiązani są do udzielania informacji telefonicznie po zweryfikowaniu tożsamości i podstaw do udzielenia informacji.
4. Przesyłanie informacji za pomocą poczty elektronicznej może nastąpić po zweryfikowaniu czy adres został wskazany Spółdzielni w oświadczeniu złożonym w formie pisemnej pod rygorem nieważności.
5. W wysyłanych pocztą elektroniczną wiadomościach stosuje się szyfrowanie danych osobowych.
6. Każdy wykonawca, zleceniobiorca, usługodawca składa oświadczenie, którego wzór stanowi **załącznik nr 10 do Polityki.**
7. Każdy najemca lub dzierżawca składa oświadczenie, którego wzór stanowi **załącznik nr 11 do Polityki.**

8. Każda osoba, której przysługuje prawo do lokalu składa oświadczenie, którego wzór stanowi **załącznik nr 12 do Polityki.**
9. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której Spółdzielnia udostępniająca dane oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności.
10. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób, naruszenie tajemnicy przedsiebiorstwa oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskującego o udostępnienie danych;
11. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych z wyłączeniem udostępnianych danych w dokumentach objętych tajemnicą na podstawie odrębnych przepisów.
12. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem RODO lub są zbędne do realizacji celu, dla którego zostały zebrane, Zarząd Spółdzielni lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 18

1. Spółdzielnia doręcza pisma wymagające dowodu doręczenia w zamkniętych kopertach przez swoich pracowników lub inne osoby posiadające upoważnienie, na adres lokalu w zasobach Spółdzielni.
2. Jeżeli jest to niemożliwe, pisma doręcza przez operatora pocztowego na adres lokalu w zasobach Spółdzielni lub na wskazany przez uprawnionego adres do doręczeń. Odbierający pismo potwierdza doręczenie swym podpisem ze wskazaniem daty doręczenia. W razie niemożności doręczenia przez operatora publicznego, przechowuje on pismo przez okres czternastu dni w swojej placówce pocztowej. Zawiadomienie o pozostawieniu pisma wraz z informacją o możliwości jego odbioru w terminie siedmiu dni licząc od dnia umieszczenia zawiadomienia w oddawczej skrzynce pocztowej. W przypadku niepodjęcia przesyłki w terminie siedmiu dni, pozostawia się powtórne zawiadomienie o możliwości odbioru przesyłki w terminie nie dłuższym niż czternaście dni od daty pierwszego zawiadomienia. Doręczenie uważa się za dokonane z upływem ostatniego dnia, a pismo pozostawia się w aktach Spółdzielni.
3. Pisma nie wymagające dowodu doręczenia w zamkniętych kopertach przez swoich pracowników lub inne osoby posiadające upoważnienie wrzuca się do skrzynek oddawczych adresatów w budynkach Spółdzielni.

Rozdział 7. Nagrywanie rozmów telefonicznych

§ 19

1. Rozmowy przychodzące do Spółdzielni mogą być nagrywane.
2. Osoba dzwoniąca do Spółdzielni będzie informowana następującym komunikatem: Spółdzielnia Mieszkaniowa „Agrodom" Szczecin *jako administrator danych osobowych informuje, że rozmowy telefoniczne są nagrywane w celu zapewnienia bezpieczeństwa i należytej obsługi interesantów. W przypadku braku zgody na nagrywanie prosimy o rozłączenie się. Informacje dotyczące przetwarzania danych osobowych znajdują się na stronie internetowej Spółdzielni w zakładce RODO oraz na tablicy informacyjnej w siedzibie Spółdzielni.*

3. Nagrania rozmów są przechowywane na nośnikach uniemożliwiających ingerencję w treść nagrań, w pomieszczeniach odpowiednio zabezpieczonych do których dostęp mają jedynie osoby posiadające upoważnienie.
4. Nagrania będą udostępniane jedynie podmiotom, które wskażą podstawę prawną i interes prawny oraz osobom, które zostały nagrane.
5. Po upływie terminu przechowywania nagrania są niszczone.

Rozdział 8 Środki techniczne i organizacyjne

§ 20.

W celu ochrony danych spełniono wymogi, o których mowa w RODO, w szczególności: przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach;
a) do przetwarzania danych zostali dopuszczeni wyłącznie pracownicy oraz osoby współpracujące ze Spółdzielnią na podstawie umów cywilnoprawnych upoważnione przez administratora danych zgodnie, które podpisały oświadczenia;
b) do przetwarzania danych zostali dopuszczeni wyłącznie członkowie organów samorządowych upoważnieni przez administratora danych, które podpisały oświadczenia;
c) osoby upoważnione do przetwarzania danych osobowych będą szkolone co najmniej raz w roku w zakresie ochrony danych osobowych;
d) zawarto umowy powierzenia przetwarzania danych;
e) została opracowana i wdrożona niniejsza Polityka.

§ 21.

W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:
a) dane osobowe przechowywane są w pomieszczeniach zabezpieczonych drzwiami wzmocnionymi zamykanymi na klucz;
b) dane osobowe przechowywane są w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej;
c) pomieszczenia, w którym przetwarzane są dane osobowe wyposażone są w system alarmowy przeciwwłamaniowy;
d) dostęp do pomieszczeń, w których przetwarzane są dane osobowe, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych;
e) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony;
f) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych na klucz szafach lub szufladach;
g) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej na klucz szafie;
h) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i wolnostojącej gaśnicy;
i) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów lub Spółdzielnia zleca zniszczenie podmiotom prowadzącym działalność gospodarczą w zakresie niszczenia dokumentów, które podpisały ze Spółdzielnią umowę o powierzenie.

§ 22.

W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
b) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych;
c) zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych;
d) dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia;
e) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;
f) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
g) użyto system Firewall do ochrony dostępu do sieci komputerowej;
h) użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

§ 23.

W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:
a) wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
b) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
c) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
d) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
e) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
f) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 24.

W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:
a) osoby upoważnione do przetwarzania danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
b) przeszkolono osoby upoważnione do przetwarzania danych osobowych w zakresie zabezpieczeń systemu informatycznego;
c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
d) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
e) kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Rozdział 9 Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 25.

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i

cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia Zarząd Spółdzielni rekomenduje wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, z uwzględnieniem, że:
1) ryzyko jest scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa ryzyka,
2) zarządzanie ryzykiem to skoordynowane działania mające na celu kierowanie Spółdzielnią i kontrolowanie organizacji pod względem ryzyka,
3) prawa i wolności osób fizycznych dotyczy przede wszystkim prawa do ochrony danych i prywatności, ale może również obejmować inne prawa podstawowe, takie jak wolność słowa, wolność myśli, swoboda poruszania się, zakaz dyskryminacji, prawo do wolności, wolność sumienia i wolność religii.
2. Oceniając, czy stopień ryzyka jest odpowiedni, Zarząd uwzględnia m.in. ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Jeżeli dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, Zarząd przed rozpoczęciem tego przetwarzania w Spółdzielni dokonuje oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi ryzyka dla ochrony danych.
4. Ogólna ocena ryzyka ma na celu określenie, czy dana operacja przetwarzania powoduje wysokie ryzyko dla ochrony danych osobowych, a w konsekwencji czy wymagane jest przeprowadzenie Oceny Skutków dla Ochrony Danych Osobowych.
5. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
6. Na podstawie wyników przeprowadzonej analizy ryzyka wdrażane są sposoby postępowania z ryzykiem.
7. Każdorazowo Zarząd Spółdzielni wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.
8. Zarząd Spółdzielni nie może zlekceważyć ryzyk, których wartość przekracza poziom minimalnego zagrożenia.
9. Przy dokonywaniu ogólnej oceny ryzyka Specjalista RODO bierze pod uwagę w szczególności:
1) użycie przy przetwarzaniu nowych technologii,
2) charakter przetwarzania,
3) zakres przetwarzania,
4) kontekst przetwarzania.

10. W szczególnych, uzasadnionych powagą zagrożeń dla ochrony Danych Osobowych przypadkach Zarząd może uznać, że należy przeprowadzić ocenę skutków dla ochrony danych dla czynności przetwarzania, mimo że nie wystąpiły dwa z powyższych czynników ryzyka.

11. Ocenę skutków dla ochrony danych wykonuje Zarząd dla:
1) jednej operacji przetwarzania,
2) wielu operacji przetwarzania – jeżeli są podobne pod względem charakteru, zakresu, kontekstu, celu i ryzyka, np. jeżeli operacja przetwarzania jest taka sama u wielu administratorów, gdy dochodzi do współadministrowania.
12. Ocena skutków dla ochrony danych zawsze jest wymagana w przypadku:
1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób

znacząco wpływających na osobę fizyczną,
2) przetwarzania na dużą skalę Danych Osobowych szczególnych kategorii lub Danych Osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa,
3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie,
4) jeżeli czynność przetwarzania znajduje się w wykazie opublikowanym przez PUODO.
13. Oceny skutków dla ochrony danych nie wykonuje się dla następujących czynności:
1) jeżeli czynność nie powoduje wysokiego ryzyka naruszenia praw i wolności osób, których dane osobowe dotyczą,
2) jeżeli czynność znajduje się w wykazie czynności przetwarzania, dla których nie jest wymagana ocena skutków dla ochrony danych opublikowanym przez PUODO,
3) gdy przeprowadzono już ocenę skutków dla ochrony danych dla podobnej czynności przetwarzania i można ją zastosować do tej operacji przetwarzania,
4) gdy czynność przetwarzania wynika z przepisów prawa i na etapie przyjmowania tych przepisów prawa dokonano już oceny skutków dla ochrony danych.

14. Ocena skutków dla ochrony danych zawiera co najmniej:
1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora,
2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

15. Z przeprowadzenia oceny skutków sporządza się raport.

16. Ocenę skutków dla ochrony danych przeprowadza Zarząd wraz z wybranymi przez siebie osobami, których określona czynność przetwarzania dotyczy.

17. Osoby przetwarzające dane osobowe są obowiązani przekazywać rzetelne, pełne i sprawdzone informacje dotyczące czynności przetwarzania, zarówno na etapie informowania o nowej czynności przetwarzania, jak i na każde zapytanie.

18. Jeżeli wynik oceny skutków dla ochrony danych wykaże, że przetwarzanie powoduje wysokie ryzyko dla ochrony danych osobowych, Zarząd wskazuje dodatkowe zabezpieczenia, które należy wdrożyć celem minimalizacji tego ryzyka. Po wdrożeniu dodatkowych zabezpieczeń Zarząd ponownie wykonuje ocenę skutków dla ochrony danych.

19. Jeżeli wynik oceny skutków dla ochrony danych wykaże, że wobec badanej czynności przetwarzania występuje wysokie ryzyko dla ochrony Danych Osobowych, którego Spółdzielnia nie może zminimalizować poprzez zastosowanie dodatkowych środków w celu zminimalizowania tego ryzyka, Specjalista RODO wstrzymuje rozpoczęcie takiego przetwarzania i informuje Kierownika o konieczności przeprowadzenia konsultacji z PUODO.

20. Po przeprowadzeniu oceny skutków dla ochrony danych Zarząd przystępuje do zarządzania zidentyfikowanym ryzykiem.

21. Zarząd analizuje zidentyfikowane ryzyko oraz wydaje odpowiednie rekomendacje:
1) jeżeli ryzyko jest niewielkie, rozważa jego akceptację,
2) jeżeli jest możliwe zminimalizowanie ryzyka poprzez wdrożenie dalszych zabezpieczeń technicznych lub organizacyjnych – zaleca ich wdrożenie,
3) jeżeli Spółdzielnia nie ma możliwości zminimalizowania ryzyka, rozważa konieczność dokonania konsultacji z osobami, których dane osobowe dotyczą oraz z PUODO.

22. Zarząd dokonuje rocznego przeglądu, testowania, mierzenia i oceniania skuteczności

stosowanych w Spółdzielni środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

23. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyka wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

24. Weryfikacja w zakresie aktualności oceny skutków dla ochrony danych jest przeprowadzana następująco:
1) ponownie przeprowadza się wszystkie ogólne oceny ryzyka zgodnie z wybraną metodyką ogólnej oceny ryzyka,
2 porównuje się wyniki z wynikami poprzednimi, opierając się na informacjach zawartych w rejestrze czynności przetwarzania,
3) jeżeli wynik ogólnej oceny ryzyka jest negatywny, Zarząd odnotowuje w rejestrze czynności przetwarzania fakt dokonania ponownej oceny ryzyka i uzyskanie wyniku negatywnego,
4) jeżeli wynik ogólnej oceny ryzyka jest pozytywny, przeprowadza się ocenę skutków dla ochrony danych, niezależnie od tego, czy ocena skutków dla ochrony danych była poprzednio przeprowadzana,
5) jeżeli ocena skutków dla ochrony danych była już poprzednio przeprowadzana dla danej czynności, analizuje się wyniki poprzedniej i obecnie dokonanej oceny skutków dla ochrony danych i ustala przyczyny różnic w wykonanej ocenie skutków dla ochrony danych,
6) Zarząd wydaje odpowiednie rekomendacje.
25. Z przeglądu sporządza się sprawozdanie.

Rozdział 10 Procedura współpracy z podmiotami zewnętrznymi

§ 26.

1. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone weryfikacją podmiotu zgodnie z wzorem stanowiącym **załącznik nr 13a do Polityki** i zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z wzorem stanowiącym **załącznik nr 13b do Polityki.**
2. Wzór wykazu podmiotów przetwarzających zawiera **załącznik nr 14 do Polityki.**
3. Nie rzadziej niż raz w roku Zarząd Spółdzielni weryfikuje zgodność z RODO wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać zgodnie z wzorem stanowiącym **załącznik nr 13c do Polityki**.
4. Wzór zgody Spółdzielni jako administratora na podpowierzenie danych osobowych zawiera **załącznik nr 13d do Polityki**.
5. Zarząd Spółdzielni udostępnia dane osobowe innemu administratorowi lub innemu wnioskodawcy, tylko wtedy, gdy spełniony jest jeden z warunków o których mowa w art. 6 ust. 1 albo w art. 9 ust. 2 RODO.
6. Udostępnianie Danych Osobowych może być dokonywane:
1) na podstawie przepisów prawa jako działanie stałe i powtarzające się, np. do Zakładu Ubezpieczeń Społecznych, Urzędów Skarbowych, Ministerstwa Finansów i innych jednostek Krajowej Administracji Skarbowej, Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych,
2) na podstawie przepisów prawa na wniosek podmiotów uprawnionych, np. Państwowej Inspekcji Pracy, Policji, sądom, innym organom ścigania, Zakładowi Ubezpieczeń Społecznych, Urzędowi Skarbowemu w ramach kontroli,
3) na wniosek innych podmiotów.
7. Każdy nowy przypadek udostępnienia danych osobowych, nieweryfikowany wcześniej przez obsługę prawną, powinien zostać zgłoszony do obsługi prawnej celem jego zweryfikowania, w

szczególności udostępnianie danych osobowych na wniosek innych podmiotów.
8. Obsługa prawna weryfikuje wszystkie okoliczności udostępniania danych osobowych, w szczególności:
1) podstawy prawne planowanego udostępnienia,
2) zakres udostępnianych danych osobowych,
3) sposób udostępnienia danych osobowych, w szczególności zapewnienie bezpieczeństwa tych danych osobowych podczas ich przekazywania.
9. Za legalność udostępnienia oraz bezpieczeństwo danych osobowych do momentu otrzymania ich przez podmiot, do którego następuje udostępnienie, odpowiada Osoba Upoważniona, która dokonuje wysyłki lub przekazania.
10. Nie udostępnia się żadnych danych osobowych drogą telefoniczną osobom spoza Spółdzielni, chyba że:
1) są to tzw. dane służbowe, tj. imię i nazwisko oraz dane służbowe pracownika: służbowy numer telefonu, służbowy adres e-mail, inne podstawowe informacje, np. godziny pracy, dane przełożonego, stanowisko, jeżeli są potrzebne do skutecznego podjęcia kontaktu służbowego z tą osobą,
2) została zastosowana procedura weryfikacji tożsamości.

Rozdział 11 Procedura domyślnej ochrony danych

§ 27.

1. Zarząd Spółdzielni w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza ocenę skutków dla ochrony danych w stosunku do tego procesu.
2. W każdym przypadku tworzenia nowego produktu lub usług Zarząd Spółdzielni uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.
3. Ocena skutków dla ochrony danych zawiera co najmniej:
a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
4. Na etapie tworzenia systemu, jego modyfikacji lub wyboru systemu, Zarząd jest obowiązany:
1) uwzględniać ochronę danych w fazie projektowania, tj. uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, wdrożyć odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych osobowych, takich jak minimalizacja danych osobowych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których Dane Osobowe dotyczą;
2) stosować domyślną ochronę danych, tj. wdrożyć odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania, w tym:
a) ilości zbieranych danych osobowych,

b) zakres ich przetwarzania,
c) okres ich przechowywania,
d) dostępności danych osobowych,
e) zabezpieczenia przed domyślnym udostępnianiem danych osobowych nieokreślonej liczbie osób fizycznych bez interwencji osoby, której dane osobowe dotyczą.

5. **Zarząd weryfikuje planowaną zmianę analogicznie do przetwarzania nowych danych osobowych, w szczególności pod względem konieczności przeprowadzenia oceny skutków oraz wydaje odpowiednie rekomendacje lub zalecenia.**

8. Zarząd uwzględnia ewentualne zmiany w odpowiednim Rejestrze czynności przetwarzania.

9. Zarzad prowadzi dokumentację systemu informatycznego, w której dokumentuje m.in.:
1) skierowanie zmiany celem przeprowadzenia weryfikacji pod względem RODO,
2) zastosowanie domyślnej ochrony Danych Osobowych.

10. Zarżad wydaje odrębną Instrukcję zarządzania zmianą w systemach informatycznych, w których uwzględnia ww. obowiązki RODO.

Rozdział 12 Procedura zarządzania naruszeniami

§ 28.

1. Każdy przebywający w obszarze przetwarzania Spółdzielni bezzwłocznie informuje o naruszeniu Zarząd Spółdzielni.
2. W każdym przypadku naruszenia ochrony danych osobowych Zarząd Spółdzielni weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Zarząd Spółdzielni w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.
4. Zarząd Spółdzielni zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
5. Zarząd Spółdzielni dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych.
6. Zarząd Spółdzielni w przypadku zaistnienia naruszenia spisuje protokół naruszenia którego wzór stanowi **załącznik nr 15 do Polityki** oraz prowadzi wykaz naruszeń, którego wzór stanowi **załącznik nr 16 do Polityki.**
7. Zarząd Spółdzielni po zaistnieniu naruszenia wdraża stosowne organizacyjne i techniczne środki naprawcze.

Rozdział 13 Procedura informowania osób

§ 29.

1. Po dokonaniu oceny legalności przetwarzania danych osobowych Zarząd Spółdzielni przygotowuje treść klauzuli informacyjnej oraz wskazuje rekomendowany sposób spełniania obowiązku informacyjnego.

2. Obowiązek informacyjny należy spełnić niezależnie od tego, czy Spółdzielnia pozyskuje je:
1) bezpośrednio od osoby, której dane osobowe dotyczą – podczas pozyskiwania tych danych osobowych, a w braku takiej możliwości (np. gdy to osoba z własnej inicjatywy przesyła swoje dane osobowe do Spółdzielni, np. w formie skargi) – niezwłocznie po otrzymaniu tych danych osobowych,
2) z innego źródła niż osoba, której dane osobowe dotyczą (np. z kancelarii notarialnej lub

urzędu miasta) – bez zbędnej zwłoki, lecz nie później niż w ciągu miesiąca od ich otrzymania. Jeżeli dane osobowe będą udostępnione innemu podmiotowi, obowiązek informacyjny należy spełnić przed dokonaniem pierwszego udostępnienia.

3. Klauzula informacyjna zawiera:
1) Pełną nazwę i dane kontaktowe Spółdzielni,
2) dane kontaktowe Inspektora Ochrony Danych, jeżeli został powołany,
3) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy realizowane przez Spółdzielnię lub przez stronę trzecią,
5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją, z rozróżnieniem na udostępnianie danych osobowych innym podmiotom, które stają się ich odrębnym administratorem oraz na ujawnianie danych osobowych podmiotom trzecim realizującym usługi w imieniu i na rzecz Spółdzielni i w tym celu przetwarzającym Dane Osobowe na podstawie zawartej umowy powierzenia przetwarzania,
6) gdy ma to zastosowanie – informacje o zamiarze przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej, o podstawie prawnej dokonania tego transferu w rozumieniu art. 45–49 RODO oraz informację o zabezpieczeniach danych osobowych i sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia,
7) okres retencji danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu, przy czym okres retencji podaje się osobno do każdego celu przetwarzania danych osobowych,
8) 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 wraz z krótkim opisem przysługujących osobie praw oraz możliwymi sposobami ich realizacji,
9) jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane osobowe dotyczą – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
10) informacje o prawie wniesienia skargi do organu nadzorczego wraz z podaniem podstawowych danych kontaktowych do PUODO,
11) Informację o tym, 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 osobowych,
12) 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 osobowe dotyczą.

4. Ponadto, jeżeli dane osobowe zostały pozyskane z innego źródła niż osoba, której one dotyczą, w klauzuli informacyjnej podaje się również:
1) informację, skąd Spółdzielnia pozyskała te dane osobowe, w tym podanie pełnej nazwy tego źródła,
2) wskazanie kategorii danych osobowych o tej osobie.

5. Obowiązek informacyjny jest spełniany:
1) w przypadku pozyskiwania danych osobowych bezpośrednio od osoby, której Dane Osobowe dotyczą – w momencie pozyskiwania tych Danych Osobowych,
2) w przypadku pozyskiwania danych osobowych z innych źródeł niż osoba, której dane osobowe dotyczą – w rozsądnym terminie, najpóźniej w ciągu miesiąca, jednak nie później niż wraz z pierwszym kontaktem z tą osobą lub z ujawnieniem danych osobowych innym

odbiorcom.

6. Dane osobowe są pozyskiwane od osoby, której dotyczą:
1) gdy ta osoba świadomie przekazuje dane osobowe, np. wypełniając formularz, przesyłając informacje, dokumenty;
2) dane osobowe są pozyskiwane z innych źródeł niż osoba, której dane osobowe dotyczą, gdy są pozyskiwane bez bezpośredniego udziału tej osoby, np.:
a) od innego administratora danych,
b) ze źródeł ogólnodostępnych, publicznych,
c) od innych osób fizycznych.

7. W razie potrzeby i po akceptacji Zarządu Spółdzielni, obowiązek informacyjny może zostać spełniony warstwowo, tj. przy użyciu klauzuli skróconej oraz pełnej, przy czym finalnie każda osoba, której dane osobowe dotyczą, musi zostać zapoznana z pełną treścią klauzuli informacyjnej.

8. Treść klauzuli skróconej zawiera co najmniej wskazanie Spółdzielni oraz cel przetwarzania danych osobowych, wskazanie praw przysługujących osobie, której dane osobowe dotyczą oraz wskazanie na pełną klauzulę informacyjną.

9. Można odstąpić od spełnienia obowiązku informacyjnego, jeżeli osoba, której Dane Osobowe dotyczą, posiada już określone informacje i jest to pisemnie udokumentowane. Zwolnienie od obowiązku informacyjnego dotyczy wyłącznie informacji, które ta osoba już posiada, natomiast w zakresie informacji, które nie zostały jeszcze osobie dostarczone, obowiązek informacyjny nadal jest aktualny i należy go spełnić.
10. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, Zarząd Spółdzielni informuje osobę, której dane dotyczą, zgodnie z **załącznikiem nr 17a do Polityki** lub umieszcza informację w umowie zgodnie z **załącznikiem nr 17b do Polityki.**
11. Wzór klauzuli informacyjnej dotyczącej ZFŚS zawiera **załącznik nr 17c do Polityki.**
12. Wzór klauzuli informacyjnej dotyczącej poczty elektronicznej zawiera **załącznik nr 17d do Polityki.**
13. Wzór klauzuli informacyjnej dotyczącej monitoringu wizyjnego zawiera **załącznik nr 17e do Polityki.**

§ 30.

W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, Zarząd Spółdzielni informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z **załącznikiem nr 18 do Polityki.**

§ 31.

W każdym wymaganym prawem przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z wzorów zgód zgodnie z **załącznikiem nr 19 do Polityki.**

Rozdział 14 Procedura użytkowania systemu informatycznego, komputerów przenośnych, poczty elektronicznej i telefonów

§ 32.

1. Pracownicy upoważnieni do przetwarzania danych osobowych i pracujący na komputerach przenośnych i telefonach zobowiązani są do przestrzegania niniejszych zasad.

2. Przetwarzanie danych osobowych na służbowych laptopach poza obszarem przetwarzania Spółdzielni może odbywać się wyłącznie po akceptacji Zarządu Spółdzielni i dostosowaniu laptopa do pracy poza siedzibą Spółdzielni, w szczególności po zabezpieczeniu laptopa odpowiednimi narzędziami szyfrującymi.
3. Dane osobowe muszą zostać zaszyfrowane na dysku i zabezpieczone hasłem.
4. Komputery i telefony przenośne są wykorzystywane do prac służbowych. W przypadku konieczności korzystania z komputera przenośnego w innym celu wszystkie dane osobowe muszą być zabezpieczone hasłem.
5. Przy przetwarzaniu danych osobowych poza obszarem przetwarzania Spółdzielni użytkownicy obowiązani są dołożyć szczególnej staranności celem zapobieżenia wglądu w przetwarzane dane osobowe innym osobom.
6. Zakazane jest użytkowanie służbowego laptopa zawierającego dane osobowe w miejscach publicznych, np. w kawiarniach, bibliotekach, kafejkach internetowych, bibliotekach publicznych, lobby hoteli, szpitali, w przestrzeni publicznej itd., chyba że wynika to ze specyfiki wykonywanego zadania i zostało zaakceptowane przez Zarząd Spółdzielni.
7. Zakazane jest podłączanie służbowych laptopów do publicznych sieci Wi-fi (HotSpot, Free Wi-fi itd.), np. w przestrzeni publicznej, w kawiarniach, hotelach, szpitalach, urzędach.
8. Użytkownik obowiązany jest dołożyć szczególnej staranności celem zapobieżenia utraty służbowych urządzeń mobilnych, w szczególności ich kradzieży, zagubienia, podpięcia przez inną osobę do tego nieuprawnioną jakichkolwiek narzędzi, w tym obcych pendrive.
9. Zakazane jest wywożenie służbowego sprzętu, na którym są lub mogą być przetwarzane dane osobowe, poza granice Unii Europejskiej, chyba że jest to niezbędne do realizacji obowiązków służbowych.
10. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie do Zarządu.
11. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera i telefonu przenośnego w czasie transportu, a przede wszystkim:

1) zaleca się przenoszenie komputera i telefonu przenośnego w odpowiedniej torbie,
2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej.

12. Gdy komputer i telefon przenośny jest pozostawiony w miejscu dostępnym dla osób nieupoważnionych, konieczne jest zabezpieczenie hasłem. Dotyczy to przede wszystkim zabezpieczenia komputera i telefonu przenośnego na stanowisku pracy, podczas przedstawiania prezentacji, szkolenia, zebrania organu Spółdzielni.
13. Użytkownik komputera i telefonu przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych
14. Pracując na komputerze i telefonie przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.
15. Zakazane jest przetwarzanie danych osobowych na urządzeniach niebędących własnością Spółdzielni lub niedopuszczonych do pracy przez Zarząd Spółdzielni.
16. Każdy użytkownik służbowego smartfona, tabletu lub telefonu komórkowego jest obowiązany stosować zabezpieczenia przed dostępem do nich osobom nieuprawnionym, w szczególności hasło dostępu. Stosowane hasła dostępu należy zmieniać w przypadku zagrożenia nieuprawnionego przejęcia.

17. Spółdzielnia umożliwia dostęp zdalny do systemów informatycznych osobom posiadającym upoważnienie do przetwarzania Danych Osobowych wyłącznie po akceptacji Zarządu Spółdzielni.
18. Umożliwianie dostępu zdalnego do sieci teleinformatycznej Spółdzielni przez podmioty trzecie jest możliwe wyłącznie w przypadku, gdy jest to niezbędne do świadczenia przez ten podmiot usług na rzecz Spółdzielni i zostanie zaakceptowane przez Zarząd Spółdzielni.
19. W przypadku umożliwiania dostępu zdalnego do systemów informatycznych podmiotom trzecim, Zarząd weryfikuje podmiot trzeci oraz planowane do stosowania narzędzia IT do dostępu zdalnego, jak również wszystkie inne czynniki mogące mieć wpływ na poziom ochrony danych osobowych w Spółdzielni.
20. Poczta elektroniczna Spółdzielni jest na bezpiecznej domenie z którą Spółdzielnia zawarła umowę o powierzenie.
21. Spółdzielnia nie umożliwia dostępu do służbowej poczty elektronicznej z innego sprzętu niż sprzęt służbowy. Każdy użytkownik jest zobowiązany korzystać z dostępu zdalnego wyłącznie ze sprzętu, który jest w jego stałym posiadaniu, jest odpowiednio zabezpieczony przed atakami pochodzącymi z sieci Internet. Zabronione jest korzystanie z dostępu zdalnego do służbowej poczty elektronicznej z obcego sprzętu komputerowego, zapamiętywanie haseł do logowania, zapisywanie jakichkolwiek załączników lub wiadomości na dyskach lokalnych komputera innego niż służbowy.
22. Zabronione jest przesyłanie danych osobowych z innych adresów e-mail niż służbowe adresy Spółdzielni.
23. Zabronione jest korzystanie z prywatnych skrzynek pocztowych do celów służbowych lub związanych z tymi celami.
24. Zabronione jest przekierowywanie służbowej poczty elektronicznej na inne niż Spółdzielni adresy e-mail.
25. Zabronione jest przesyłanie danych osobowych innych niż dane kontaktowe publiczną siecią Internet w sposób niezabezpieczony, chyba że odbiorca wyraźnie zażyczy sobie dokonania takiej wysyłki, po uprzednim poinformowaniu jej o ryzykach związanych z przesyłaniem niezabezpieczonej poczty elektronicznej publiczną siecią Internet oraz o możliwości wysłania danych osobowych w formie zaszyfrowanej odpowiednio złożonym hasłem.

Rozdział 15 Przetwarzanie danych osobowych w rejestrze członków

§ 33

1. Rejestr członków Spółdzielni, zwany dalej rejestrem, zawiera następujące dane określone w art. 30 Prawa spółdzielczego oraz w Statucie Spółdzielni.
2. Rejestr jest prowadzony w wersji papierowej przez pracownika, który działa w imieniu Zarządu na podstawie udzielonego przez Zarząd pełnomocnictwa i upoważnienia do przetwarzania danych osobowych.
3. Rejestr członków w wersji papierowej jest przechowywany w zamkniętej na wzmocniony zamek szafie. Klucz do szafy jest przechowywany zgodnie z Polityką kluczy.
4. Rejestr członków prowadzony w wersji elektronicznej zawiera niezbędne zabezpieczenia techniczne i spełnia wszystkie wymogi prawne, co zostało potwierdzone przez obsługę informatyczną Spółdzielni.
5. Dostęp do rejestru członków ma Pracownik, który odpowiada za zabezpieczenie rejestru oraz Zarząd Spółdzielni.
6. Do przeglądania rejestru członków uprawnieni są:
1) Członkowie Spółdzielni, po weryfikacji członkostwa;

2) Małżonek członka, w zakresie danych małżonka po okazaniu odpisu zupełnego aktu małżeństwa wraz z pisemnym oświadczeniem, że dane w odpisie aktu się nie zmieniły;
3) Wierzyciele członków, w zakresie danych dłużnika, lub wierzyciele Spółdzielni po okazaniu dokumentu udowadniającego wymagalną wierzytelność.
7. Osoby wymienione w ustępie 6 okazują dokument tożsamości celem weryfikacji tożsamości.
8. Osobom wymienionym w ustępie 6 okazywana jest klauzula informacyjna zgodnie z art. 13 RODO.
9. Rejestr jest udostępniany w siedzibie Spółdzielni przez Pracownika, który odpowiada za weryfikację osób uprawnionych do przeglądania.
10. Rejestr jest przeglądany przez osobę uprawnioną w obecności Pracownika.
11. Osoba uprawniona do przeglądania rejestru nie jest uprawniona do robienia kopii, zdjęć oraz notatek.
12. Rejestr jest sprawdzany przez odpowiedzialnego pracownika po zwrocie.
13. Pracownik prowadzi wykaz udostępniania rejestru do przeglądania, którego wzór stanowi **załącznik nr 20** do Polityki.

Rozdział 16 Procedura realizacji praw osób

§ 34.

1. Osoby, których dane dotyczą składają żądania dotyczące swoich praw w formie umożliwiającej ich identyfikację.
2. Zarząd weryfikuje tożsamość wnioskodawców określonych w ust. 1. W przypadku braku możliwości jednoznacznej weryfikacji tożsamości wnioskodawcy, Zarząd Spółdzielni może żądać dodatkowych informacji w celu weryfikacji tożsamości.
3. Rozpoznanie żądania zgłoszonego przez pełnomocnika wnioskodawcy jest możliwe pod warunkiem, że przedstawia on pełnomocnictwo, z którego jednoznacznie wynika umocowanie do zgłoszenia żądania i zakres żądania.
4. W przypadku braku możliwości jednoznacznego określenia faktycznej treści żądania Wnioskodawcy Zarząd Spółdzielni może żądać od wnioskodawcy dodatkowych wyjaśnień.
5. W przypadku wątpliwości co do tożsamości wnioskodawcy lub treści żądania Zarząd informuje o przedłużeniu terminu udzielenia odpowiedzi.
6. Zarząd Spółdzielni lub osoba upoważniona przez Zarząd rejestruje każde otrzymane żądanie w rejestrze stanowiącym Załącznik nr 21 do Polityki.
7. Zarząd Spółdzielni po weryfikacji określonej w powyższych ustępach, niezwłocznie, nie później niż w terminie miesiąca, realizuje prawa osób, których dane dotyczą, w szczególności:
- prawo do informacji o przetwarzaniu;
- prawo do uzyskania kopii danych;
- prawo dostępu do danych;
- prawo do sprostowania danych;
- prawo do usunięcia danych;
- prawo do przenoszenia danych,
- prawo do sprzeciwu wobec przetwarzania danych,
- prawo do wycofania zgody.
8. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w RODO Zarząd Spółdzielni rozpatruje indywidualnie i odpowiada pisemnie.
9. Przedłużenie terminu do realizacji praw RODO może zostać dokonane o maksymalnie dwa miesiące z uwagi na:
1) skomplikowany charakter żądania,
2) liczbę żądań złożonych przez tę osobę.

10. W ciągu miesiąca od złożenia wniosku Specjalista RODO kieruje odpowiedź do osoby, która złożyła wniosek, informując ją o:
1) realizacji jej prawa,
2) odmowie realizacji jej prawa wraz z informacją o przyczynie odmowy oraz o możliwości złożenia skargi do PUODO i podstawowymi danymi kontaktowymi PUODO,
3) przedłużeniu terminu do realizacji wniosku wraz z informacją o przyczynie odmowy oraz o możliwości złożenia skargi do PUODO i podstawowymi danymi kontaktowymi PUODO.

11. Każda osoba, której dane osobowe dotyczą, posiada następujące prawa:
1) prawo do cofnięcia zgody – może cofnąć wyrażoną przez siebie zgodę w każdym momencie i bez podawania przyczyny (art. 7 RODO);
2) prawo dostępu – może żądać od Spółdzielni informacji o przetwarzaniu jej danych osobowych, tj. potwierdzenia, czy przetwarzane są jej dane osobowe. Jeżeli dane o osobie są przetwarzane, jest ona uprawniona do uzyskania dostępu do nich, uzyskania ich kopii oraz do uzyskania następujących informacji: o celach przetwarzania, kategoriach danych osobowych, informacji o odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione, o okresie przechowywania danych lub o kryteriach ich ustalania, o przysługujących osobie prawach związanych z przetwarzaniem jej danych osobowych, o możliwości wniesienia skargi do organu nadzoru, o źródle pozyskania danych osobowych, jeżeli nie zostały pozyskane bezpośrednio od osoby, której dane dotyczą, oraz o profilowaniu i zautomatyzowanym przetwarzaniu decyzji (art. 15 RODO);
3) prawo do sprostowania – może sprostować dane osobowe jej dotyczące. Jeżeli osoba uzyska informację o tym, że jej dane osobowe przetwarzane przez Spółdzielnię są nieprawidłowe, nieaktualne lub niekompletne, ma ona prawo żądać ich niezwłocznego sprostowania lub uzupełnienia (art. 16 RODO);
4) prawo do zapomnienia – może żądać usunięcia jej danych osobowych, przy czym, jeżeli osoba wyraziła zgodę na przetwarzanie danych osobowych, żądanie usunięcia odniesie taki sam skutek jak cofnięcie zgody (art. 17 RODO);
5) prawo do ograniczenia przetwarzania – może żądać ograniczenia przetwarzania danych osobowych (art. 18 RODO), tj. zażądać zaprzestania ich przetwarzania z wyjątkiem ich przechowywania, w sytuacjach, gdy:
a) osoba, której dane Dotyczą, kwestionuje prawidłowość danych osobowych na okres, w którym Spółdzielnia będzie weryfikowała ich prawidłowość,
b) osoba, której Dane dotyczą, kwestionuje zgodność z prawem przetwarzania danych osobowych przez Spółdzielnię,
c) Spółdzielnia nie potrzebuje już tych danych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony jego roszczeń,
d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu podjęcia decyzji przez Spółdzielnię co do zasadności sprzeciwu;
6) prawo do wniesienia sprzeciwu – może wnieść sprzeciw wobec przetwarzania jej danych osobowych w prawnie uzasadnionych celach Spółdzielni;
7) prawo do przenoszenia – może przenieść swoje dane osobowe, tj. otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe, które dostarczyła Spółdzielni, jeżeli ich przetwarzanie odbywa się na podstawie zgody, lub zażądać przesłania tych danych innemu, wskazanemu przez osobę, której dane dotyczą, administratorowi (art. 20 RODO).

12. Jeżeli Zarząd Spółdzielni ma wątpliwości, czy i w jakim zakresie określony wniosek powinien zostać zrealizowany, kieruje zapytanie do obsługi prawnej Spółdzielni.

13. Każdy wniosek jest interpretowany zgodnie z życzeniem osoby, której dane osobowe dotyczą, niezależnie od jego literalnego brzmienia. Jeżeli Zarząd Spółdzielni ma wątpliwości

co do intencji lub zamierzonego celu wniosku, kontaktuje się z osobą, której dane osobowe dotyczą, celem ich wyjaśnienia.

14. Każdy kontakt z osobą, której dane osobowe dotyczą, odbywa się zgodnie z zasadą transparentności i w celu ułatwienia osobie realizacji jej praw.

15. Kontakt z osobą, której dane osobowe dotyczą, odbywa się:
1) na etapie wyjaśniania wniosku – najskuteczniejszym i najszybszym sposobem dostępnym w konkretnym przypadku,
2) na etapie realizacji wniosku – pisemnie, chyba że osoba kontaktuje się elektronicznie i nie zastrzegła innej formy odpowiedzi – wówczas należy kontaktować się z osobą elektronicznie.

16. Przy realizacji praw RODO, z którymi wiąże się ujawnienie danych osobowych w odpowiedzi na wniosek (w szczególności prawo do otrzymania kopii danych osobowych, prawo do przenoszenia danych osobowych), Zarząd Spółdzielni upewnia się, że podczas ich przekazywania do osoby, której dane osobowe dotyczą, lub do innego administratora wskazanego przez tę osobę, dane osobowe są odpowiednio zabezpieczone, w szczególności przez tajemnicę korespondencji lub zaszyfrowanie danych osobowych lub ich elektronicznego nośnika.

17. Jeżeli osoba, której dane osobowe dotyczą, kontaktuje się elektronicznie lub wniosła o wysłanie odpowiedzi drogą mailową, osoba upoważniona przez Zarząd, zabezpiecza dane osobowe indywidualnym hasłem.

18. Można przekazać w tym samym mailu instrukcje, jak hasło zostało skonstruowane, bez podawania samego hasła (np. informacja, że hasło składa się z numeru PESEL).

19. Zarząd Spółdzielni może nałożyć opłatę za realizację prawa, jeżeli:
1) osoba złożyła drugi lub kolejny wniosek o prawo otrzymania kopii danych osobowych – w wysokości kosztów wydania kopii,
2) żądanie jest ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter – w wysokości kosztów udzielenia informacji, kontaktów z wnioskodawcą i podjęcia żądanych działań.
20. Zarząd Spółdzielni może odmówić realizacji prawa, jeżeli:
1) wniosek został złożony w zakresie przekraczającym prawa RODO,
2) Spółdzielnia nałożyła opłatę za jego realizację i poinformował o tym osobę, której dane osobowe dotyczą, lecz osoba nie uiściła opłaty,
3) żądania osoby są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter.

21. Pracownik prowadzący dziennik korespondencyjny, któremu osoba, której dane dotyczą, złożyła wniosek, jest obowiązany odnotować datę złożenia wniosku i przekazać go Zarządowi Spółdzielni. Jeżeli wniosek został złożony ustnie (osobiście lub telefonicznie), Pracownik odbiera od osoby składającej wniosek jej imię i nazwisko oraz co najmniej jedną daną kontaktową (numer telefonu, adres e-mail, adres korespondencyjny) oraz treść żądania, utrwala te informacje papierowo lub elektronicznie i niezwłocznie przekazuje je Zarządowi Spółdzielni.

22. Pracownik prowadzący dziennik korespondencyjny ma obowiązek potwierdzić tożsamość osoby wnioskującej przed realizacją wniosku. Potwierdzenie tożsamości osoby wnioskującej odbywa się z użyciem danych osobowych przetwarzanych przez Spółdzielnię o osobie, której dane osobowe dotyczą.

23. Potwierdzenie tożsamości powinno polegać na potwierdzeniu imienia i nazwiska osoby wnioskującej oraz na weryfikacji tożsamości poprzez zadanie osobie po jednym, a jeżeli jest to możliwe ze względu na zakres informacji przetwarzanych o tej osobie – po dwa pytania z zakresu tego, kim ta osoba jest np. Nr PESEL, adres lokalu w zasobach Spółdzielni, adres e-mail podany do kontaktu, numer identyfikacyjny.

24. Jeżeli osoba, której Dane Osobowe dotyczą, składa taki sam wniosek o to samo prawo przed upływem 6 miesięcy od rozpatrzenia poprzedniego wniosku i od czasu ostatniej realizacji takiego samego wniosku nie zmieniły się żadne okoliczności przetwarzania danych osobowych tej osoby, Zarząd Spółdzielni może:
1) odmówić realizacji prawa i poinformować, że zakres czynności przetwarzania lub zakres Danych Osobowych nie uległ zmianie,
2) nałożyć rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań.

§ 35.

Jeżeli Zarząd Spółdzielni nie podejmuje działań w związku z żądaniem wnioskodawcy to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje wnioskodawcę o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do Prezesa UODO lub skorzystania ze środków ochrony prawnej przed sądem. Odmowa podjęcia działań w związku ze zgłoszonym żądaniem dopuszczalna jest w przypadku gdy żądanie jest ewidentnie nieuzasadnione lub nadmierne.

§ 36.

W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych Zarząd Spółdzielni niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

§ 37.

Zarząd Spółdzielni odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów RODO, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z RODO.

Rozdział 17 Zapewnienie ciągłości zgodności

§38

1. Zarząd Spółdzielni zapewnia stałe utrzymywanie zgodności działania Spółdzielni z wymaganiami ochrony danych osobowych przewidzianymi w RODO, w tym weryfikuje i optymalizuje wdrożone w organizacji rejestry i procedury.
2. W tym celu Zarząd Spółdzielni między innymi monitoruje zmiany w przepisach prawa, wytyczne krajowych i międzynarodowych organów ochrony danych osobowych oraz orzecznictwo sądów i trybunałów, a także uwzględnia najlepsze „dobre praktyki".
3. W Spółdzielni identyfikuje się elementy istotne dla ciągłości działania danych osobowych:
1) dostępność danych osobowych:
a) dostępność baz danych osobowych,
b) dostępność systemów informatycznych służących do przetwarzania danych osobowych,
c) dostępność infrastruktury zapewniającej działanie baz i systemów informatycznych;
2) dostępność zasobów ludzkich:
a) dostępność pracowników Spółdzielni,
b) dostępność obsługi serwisowej świadczonej przez firmy zewnętrzne,
c) dostępność stanowisk pracy;
3) dostępność siedziby,
4) dostępność narzędzi pracy.
4. W ramach zarządzania ciągłością działania danych osobowych Zarząd Spółdzielni podejmuje działania:

1) prewencyjne, mające na celu ograniczenie ryzyk oraz przygotowanie Spółdzielni na wystąpienie zagrożeń, tj. przygotowanie poszczególnych scenariuszy incydentów i procedur postępowania z incydentami,
2) reagowanie na incydenty ciągłości działania, czyli podejmowanie działań po zaistnieniu incydentu ciągłości działania,
3) przywracanie normalnego trybu działania,
4) podejmowanie działań minimalizujących ryzyko wystąpienia incydentu w przyszłości.

5. Działania prewencyjne podejmowane przez Spółdzielnię to:
1) sporządzanie kopii zapasowych danych osobowych,
2) sporządzanie kopii systemów służących do ich obsługi,
3) przygotowanie na wypadek braku dostępności standardowej infrastruktury teleinformatycznej i usług,
4) przygotowanie na wypadek braku dostępności infrastruktury fizycznej Spółdzielni,
5) przygotowanie na wypadek braku kluczowych zasobów ludzkich w Spółdzielni,
6) przygotowanie na wypadek braku dostępności do standardowej obsługi zewnętrznej kluczowych zasobów.

6. Działania prewencyjne mogą polegać na:
1) stałym zapewnieniu rozwiązań alternatywnych, np. posiadanie kopii zapasowych, posiadanie rozwiązań UPS pozwalających na czasowe zapewnienie działania Spółdzielni niezależnie od braku dostępu do infrastruktury lub usług, zawarta umowa ramowa na obsługę, z której Spółdzielnia, co do zasady, nie korzysta, ale w razie potrzeby może korzystać w każdej chwili, drugie lub kolejne równorzędne konto bankowe w innym banku zasilone dostępnymi finansami zapewniającymi płynność finansową przez określony czas;
2) przygotowaniu Spółdzielni do szybkiego zapewnienia rozwiązań alternatywnych, tj. posiadania aktualnej listy rozwiązań i dostawców alternatywnych wraz z warunkami ewentualnej współpracy w trybie nagłym odpowiadającymi ewentualnym potrzebom i możliwościom Spółdzielni, z którymi w razie potrzeby Spółdzilenia jest w stanie podjąć współpracę niezwłocznie.

7. Zarządzanie incydentem ciągłości działania należy do obowiązków Zarządu Spółdzielni.

8. Wszystkie działania podejmowane w ramach zarządzania incydentem ciągłości działania danych osobowych są wykonywane z najwyższym priorytetem czasowym, niezależnie od czasu jego zaistnienia, w tym również po godzinach pracy.

9. O zastosowaniu konkretnego rozwiązania awaryjnego decyduje Zarząd Spółdzielni.

10. W celu zapewnienia możliwości odtworzenia danych osobowych oraz systemów służących do ich przetwarzania na wypadek utraty danych osobowych lub systemów, utraty możliwości dostępu do nich lub utraty integralności danych osobowych Spółdzielnia zapewnia wykonywanie kopii zapasowych pozwalających na odtworzenie każdego zasobu zawierającego dane osobowe.

11. Zarząd wykonuje kopie zapasowe:
1) baz Danych Osobowych,
2) zasobów sieciowych,
3) poczty elektronicznej,
4) dysków lokalnych,
5) systemów informatycznych służących do przetwarzania danych osobowych.

12. Kopie zapasowe doraźne wykonuje się również przed każdą znaczącą pracą serwisową dotyczącą systemu lub bazy danych osobowych.

13. Kopie zapasowe przechowuje się w innym miejscu niż fizyczne nośniki danych, których kopie dotyczą, oddalonym w sposób zapewniający odseparowanie ich od zagrożeń fizycznych

dotyczących tych danych (np. w przypadku powodzi, pożaru, kradzieży, zniszczenia).

14. **Zarząd** wykonuje próby odtworzeniowe trzech losowo wybranych kopii zapasowych co najmniej raz w miesiącu.

15. Zarząd prowadzi:
1) rejestr kopii zapasowych,
2) rejestr nośników kopii zapasowych,
3) rejestr wykonywanych prób odtworzeniowych.

16. Na wypadek braku dostępności do systemów informatycznych służących do przetwarzania danych osobowych Spółdzielnia zapewnia stosowanie awaryjnych systemów informatycznych.

17. **Zarząd** zapewnia rezerwowe systemy informatyczne na wypadek nagłej i nieoczekiwanej niemożności korzystania z obecnie stosowanych systemów informatycznych. W tym celu **Zarząd** prowadzi wykaz awaryjnych systemów mogących zastąpić stosowane systemy wraz z instrukcją ich szybkiego pozyskania.

18. W przypadku braku dostępności do sprzętu komputerowego użytkowników dopuszczalne jest czasowe zezwolenie na pracę z użyciem prywatnego sprzętu komputerowego użytkowników. **Zarząd** zapewnia możliwości techniczne tymczasowego przekierowania pracy na komputery prywatne użytkowników, a jeżeli nie jest to możliwe, zapewnia przekierowanie pracy użytkowników kluczowych.

19. Na wypadek czasowej niedostępności do miejsc pracy Spółdzielni dla osób upoważnionych, Spółdzielnia zapewnia lokalizację zastępczą np. praca w domu osób upoważnionych. Dopuszczalne jest czasowe przekierowanie pracy na system pracy zdalnej pod warunkiem zapewnienia użytkownikom dostępu do kluczowych systemów umożliwiających im wykonywanie pracy.

20. W ramach działań prewencyjnych na czas krótkotrwałej nieobecności pracowników (urlop planowany, urlop zdrowotny i okolicznościowy) Zarząd Spółdzielni w zakresie czynności wskazuje zastępstwo dla każdego stanowiska pracy.

21. Zarząd Spółdzielni zapewnia, aby plan urlopów wypoczynkowych przewidywał możliwość stosowania zastępstwa zgodnie z zakresem czynności pracowników. Niedozwolona jest akceptacja urlopu wypoczynkowego dla osoby, która w tym samym czasie zastępuje już inną nieobecną osobę, chyba że ma miejsce szczególnie uzasadniony przypadek, a zastępstwo zostanie zapewnione przez inną osobę.

22. Zarząd Spółdzielni dokłada szczególnej staranności, aby wakat na stanowiskach kluczowych utrzymywał się jak najkrócej.

Rozdział 18 Kontrola i współpraca z Prezesem UODO

§39

1. Wewnętrzna kontrola z zakresu ochrony danych osobowych może być przeprowadzona przez Zarząd Spółdzielni.
2. Kontrola z zakresu ochrony danych osobowych może być przeprowadzona wyłącznie przez upoważnionego pracownika Urzędu Ochrony Danych Osobowych, zwanego dalej „kontrolującym". Do kontroli stosuje się przepisy RODO, ustawy o ochronie danych osobowych i Kodeksu postępowania administracyjnego.
3. Kontrolę przeprowadza się po okazaniu przez kontrolującego imiennego upoważnienia wraz z legitymacją służbową.
4. W postępowaniu kontrolnym uczestniczy Zarząd Spółdzielni.

5. Kontrolującemu należy zapewnić warunki i środki niezbędne do sprawnego przeprowadzenia kontroli.
6. Kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.
7. Wszystkie osoby zatrudnione w Spółdzielni są zobowiązane do współpracy z kontrolującym w postępowaniu kontrolnym, w tym składania wyjaśnień, okazywania dokumentów i umożliwiania dostępu do pomieszczeń i sprzętu służącego do przetwarzania danych osobowych.
8. Z czynności kontrolnych kontroler sporządza protokół, którego jeden egzemplarz doręcza Spółdzielni.
9. Protokół podpisują kontrolujący i Zarząd Spółdzielni. W razie odmowy podpisania protokołu przez kontrolowanego kontrolujący czyni o tym wzmiankę w protokole. Przed podpisaniem protokołu Spółdzielnia może w terminie 7 dni od przedstawienia mu protokołu do podpisu złożyć pisemne zastrzeżenia do tego protokołu.
10. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli, Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania. Na podstawie ustaleń kontroli Prezes Urzędu może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym uchybień i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach. W razie stwierdzenia, że działanie lub zaniechanie wyczerpuje znamiona przestępstwa określonego w ustawie, Prezes Urzędu kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.
11. Każda osoba, której prawa przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, może żądać, zaniechania tego działania a także może żądać ażeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków.
12. Zarząd Spółdzielni występuje z wnioskiem o konsultacje do Prezesa UODO w sytuacji, w której w wyniku przeprowadzonej oceny skutków dla ochrony danych na liście badanych operacji przetwarzania znajdą się operacje, dla których ryzyko naruszenia praw i wolności oszacowane zostało jako wysokie i Zarząd Spółdzielni nie może znaleźć wystarczających środków do zmniejszenia tego ryzyka do dopuszczalnego poziomu. Do konsultacji stosuje się przepisy RODO, ustawy o ochronie danych osobowych i Kodeksu postępowania administracyjnego.

Rozdział 19 Postanowienia końcowe

§ 40

Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą. Osoby nie przestrzegające przepisów o ochronie danych osobowych podlegają odpowiedzialności karnej, dyscyplinarnej i odszkodowawczej.

§ 41

1. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa stosuje się przepisy o ochronie danych osobowych.
2. Polityka ochrony danych przyjęta została Uchwałą Zarządu Spółdzielni z dnia **8.03.2021** roku i obowiązuje od dnia jej przyjęcia.

Dariusz Wociór
RADCA PRAWNY