POLITYKA OCHRONY DANYCH W SPÓŁDZIELNI Budowlano-Mieszkaniowej ZACHÓD z siedzibą : 00-801 Warszawa , ul.Chmielna 116/118 .

Rozdział 1 Postanowienia ogólne

§ 1.

Ilekroć w dokumencie jest mowa o:

1) **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);
2) **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;
3) **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;
4) **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;
5) **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**;
6) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8) **administrator , zwanym także ADO**– rozumie się przez to Spółdzielnię Budowlano-Mieszkaniową ZACHÓD z siedzibą : 00-801 Warszawa , ul.Chmielna 116/118 (**zwaną dalej Spółdzielnią**), który 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;
9) **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;

10) **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;
11) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
12) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
13) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
14) **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;
15) **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;
16) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;
17) **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;
18) **ASI** – osoba pełniąca funkcję w Spółdzielni koordynatora ds. systemu informatycznego w zakresie ochrony danych osobowych;
Koordynator ds. ochrony danych osobowych – osoba odpowiedzialna za koordynowanie realizacji przez Spółdzielnię praw i obowiązków z zakresu ochrony danych osobowych;

§ 2.

1.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,
2. 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.

Rozdział 2 Administrator danych

§ 3.

1. Administratorem danych jest Spółdzielnia Budowlano-Mieszkaniowa ZACHÓD z siedzibą : 00-801 Warszawa , ul.Chmielna 116/118 .
2. W imieniu administratora danych w zakresie stosowania przepisów o ochronie danych osobowych oraz wewnętrznych procedur działa Zarząd Spółdzielni Budowlano-Mieszkaniowej ZACHÓD z siedzibą : 00-801 Warszawa , ul.Chmielna 116/118 .

3. Administrator danych w szczególności:
   - 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.
   - Prowadzi rejestr czynności przetwarzania.
   - Wyznacza koordynatora ds. ochrony danych osobowych oraz zastępców koordynatora ds. ochrony danych osobowych .Administrator Systemu Informatycznego w Spółdzielni Budowlano-Mieszkaniowej ZACHÓD powołał na stanowisko koordynatora ds.ochrony danych osobowych Magdalenę Mossoczy oraz zastępcę koordynatora ds.ochrony danych osobowych Ewę Fronczak .
4. Do kompetencji koordynatora ds. ochrony danych osobowych należy w szczególności:
   1) zapewnianie zapoznania i informowanie administratora, 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 oraz opracowywanie w tym zakresie sprawozdań dla Administratora,
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 we współpracy z ASI w zakresie dotyczącym systemu IT,
8) nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych, środki ich ochrony oraz przestrzegania zasad w niej określonych,
9) wnioskowanie i opiniowanie wniosków do ADO o 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 we współpracy z ADO, w których przetwarzane są dane osobowe oraz organizacją kontroli przebywających w nich osób,
11) zapewnienie przeciwdziałania incydentom oraz prowadzenie rejestru incydentów i zagrożeń,

5. Do kompetencji zastępcy Koordynatora ds. ochrony danych osobowych należy:
1) monitorowanie przestrzegania RODO, innych przepisów o ochronie danych oraz niniejszej Polityki, w tym działania zwiększające świadomość na wyznaczonym terenie;
2) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania na wyznaczonym terenie;
3) współpraca z IOD;
4) pełnienie funkcji punktu kontaktowego między IOD a pracownikami na wyznaczonym terenie.
5) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie sprawozdań dla IOD,
6) 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 we współpracy z ASI w zakresie dotyczącym systemu IT na wyznaczonym terenie,
7) wnioskowanie i opiniowanie wniosków do IOD o 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 na wyznaczonym terenie,
8) nadzór nad fizycznym zabezpieczeniem pomieszczeń we współpracy z IOD, w których przetwarzane są dane osobowe oraz organizacją kontroli przebywających w nich osób na wyznaczonym terenie,
9) zapewnienie przeciwdziałania incydentom oraz prowadzenie rejestru incydentów i zagrożeń na wyznaczonym terenie,

6. Do zadań ASI należy zapewnienie działania infrastruktury teleinformatycznej
i oprogramowania w sposób zapewniający właściwy poziom bezpieczeństwa informacji wynikający z obowiązujących przepisów i procedur wewnętrznych;
7. Nadzorowanie przez ASI 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 ASI 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 raportowanie do IOD 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 Administratora o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych w systemie IT oraz realizacja tych czynności po akceptacji Administratora,
    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.

Rozdział 3 Przetwarzanie danych osobowych

§ 4.

1 Zasady przetwarzania danych osobowych:

1) dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Spółdzielnia może żądać podania jedynie tych danych, które są niezbędne do realizacji jej celów i zadań,

2) zakres danych osobowych przetwarzanych przez jednego Użytkownika w systemie IT nie może być szerszy niż powierzony do przetwarzania w związku z wykonywanymi przez niego obowiązkami,

3) po wykorzystaniu, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą, zniszczone lub, w przypadku powierzenia, zwrócone podmiotowi, który dane powierzył;

2. Zasady ochrony danych osobowych określone przez Politykę mają zastosowanie do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów przetwarzania informacji zawierających dane osobowe, w tym systemów IT,
2) informacji będących własnością Spółdzielni oraz przetwarzanych przez nią w związku z prowadzoną działalnością,
3) wszystkich lokalizacji, budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
4) wszystkich osób świadczących pracę lub wykonujących czynności na rzecz Spółdzielni mających dostęp do informacji podlegających ochronie,

§ 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 administracji.

§ 6.

1. Obszarem przetwarzania danych osobowych są wydzielone pomieszczenia lub części pomieszczeń w siedzibie Spółdzielni Budowlano-Mieszkaniowej Zachód znajdującej się przy ul. Śliskiej 10 w Warszawie **(załącznik nr 1 do Polityki).**

2. Nadzór nad dostępem do pomieszczeń, w których przetwarzane są dane osobowe sprawuje : ..... .

3. Pracownicy i inne osoby przebywające w obszarze przetwarzania są zobowiązani do informowania Koordynatora ds. ochrony danych osobowych lub Zastępcy Koordynatora ds.ochrony danych osobowych o zauważonych próbach nieuprawnionego dostępu do pomieszczeń, o których mowa w ust. 1.

4. Po godzinach urzędowania dostęp do pomieszczeń mają pracownicy oraz osoby upoważnione pisemnie przez Administratora.
5. ADO w porozumieniu z Inspektorem Ochrony Danych oraz ASI może określić pomieszczenia, do których dostęp osób sprzątających i innych będzie ograniczony i możliwy tylko pod nadzorem osób uprawnionych do przebywania w tych pomieszczeniach.
6. Osoby opuszczające pomieszczenie, 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.
7. Zabrania się samowolnego dorabiania kluczy oraz ich wynoszenia poza siedzibę
Spółdzielni. Każdorazowa potrzeba dorobienia dodatkowego klucza lub kluczy winna być zgłoszona Administratorowi, który wyraża na to pisemną zgodę oraz określa zasady wykonania raz posługiwania się kopią klucza/kluczy.
8. 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 zbędne
w postaci błędnie utworzonej lub niepotrzebnej dokumentacji mającej krótkotrwałe znaczenie praktyczne, m.in. wydruków komputerowych i innych materiałów analogowych zawierających dane osobowe.

§ 7.

1. Wszystkie osoby, które posiadają dostęp do danych osobowych w obszarze wymienionym w § 6 muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez ADO oraz podpisać oświadczenie o zachowaniu poufności.
2. Wzór upoważnienia dla pracowników oraz osób współpracujących ze Spółdzielni na podstawie umów cywilnoprawnych, którego wzór stanowi **załącznik nr 2 do Polityki.**
3. Wzór oświadczenia o zachowaniu poufności dla pracowników oraz osób współpracujących ze Spółdzielni na podstawie umów cywilnoprawnych, którego wzór stanowi **załącznik nr 3 do Polityki.**
4. Wzór upoważnienia dla osób będących członkami Rady Nadzorczej i członkami innych organów samorządowych w Spółdzielni, którego wzór stanowi **załącznik nr 4 do Polityki**.
5. Wzór oświadczenia o zachowaniu poufności dla osób będących członkami Rady Nadzorczej w Spółdzielni, którego wzór stanowi **załącznik nr 5 do Polityki**.
6. Zakres upoważnień określonych w powyższych ustępach został określony na podstawie Rejestru czynności przetwarzania danych osobowych, którego wzór stanowi załącznik **nr 6 do Polityki**.
7. Koordynator ds. ochrony danych osobowych lub Zastępca Koordynatora ds.ochrony danych osobowych prowadzi rejestr czynności przetwarzania danych osobowych zgodnie z art. 30 ust. 1 RODO.
8. Koordynator ds. ochrony danych osobowych lub Zastępca Koordynatora ds.ochrony danych osobowych prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora zgodnie z art. 30 ust. 2 RODO, którego wzór stanowi **załącznik nr 7 do Polityki.**
9. Ewidencja osób upoważnionych jest prowadzona zgodnie z wzorem stanowiącym **załącznik nr 8 do Polityki**.

10. Każdy pracownik w zakresie czynności wykonywanych na stanowisku pracy prowadzi:
- wykaz udostępnień danych innym podmiotom, którego wzór stanowi **załącznik nr 9 do Polityki,**
- wykaz udostępnień danych osobowych osobom, których dotyczą, którego wzór stanowi **załącznik nr 10 do Polityki.**
11. 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 11 do Polityki.**

§ 8.

Uprawnienia do przetwarzania danych osobowych w systemach IT nadawane są zgodnie z właściwą procedurą określoną w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Spółdzielni Budowlano-Mieszkaniowej ZACHÓD z siedzibą : 00-801 Warszawa , ul.Chmielna 116/118 **.** 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 przesyłką rejestrowaną, a w przypadku danych zawartych na nośnikach magnetycznych, optycznych lub elektronicznych – przesyłką rejestrowaną za potwierdzeniem odbioru;
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 znanych 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.

Rozdział 4. Monitoring wizyjny

§ 12.

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.
4. Decyzję o zamontowaniu kamer podejmuje Zarząd.
3. Zarząd odpowiada za zabezpieczenie, funkcjonowanie monitoringu oraz przechowywanie i udostępnianie nagrań monitoringu oraz niszczenie (usuwanie) nagrań.
4. Teren objęty zakresem monitoringu powinien być oznaczony tabliczkami informującymi, że Spółdzielnia monitoruje teren i nagrywa obraz. Na tablicach informacyjnych powinny być wywieszone klauzule informacyjne w zakresie przetwarzania danych w monitoringu wizyjnym.

§ 13

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.

§ 14

1. Dane pochodzące z nagrań kamer wideo 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 oraz instytucje państwowe i samorządowe po wskazaniu podstaw prawnych, faktycznych i interesu prawnego. Nagrania nie powinny być udostępniane osobom fizycznym gdyż nie można zweryfikować czy nagrania zostaną przez te osoby użyte zgodnie z prawem, chyba że jest możliwe udostępnienie fragmentu nagrania, które obejmuje osobę której wniosek dotyczy. Osoba fizyczna powołując się na nagrania monitoringu może złożyć wniosek dowodowy do odpowiedniej instytucji, ze zobowiązaniem Spółdzielni do udostępnienia odpowiedniej instytucji nagrań.

Rozdział 5. Obsługa interesantów, doręczanie korespondencji, udostępnianie informacji

§ 15

1. Przed udzieleniem informacji bezpośredniej tożsamość interesantów powinna być zweryfikowana poprzez żądanie okazania dokumentu tożsamości celem sprawdzenia uprawnień dostępu do danych osobowych.
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. Każda osoba, której przysługuje prawo do lokalu składa oświadczenie, którego wzór stanowi **załącznik nr 12 do Polityki.**
7. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której administrator danych udostępniający dane oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności;
8. 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 oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskującego o udostępnienie danych;
9. 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;
10. 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, ADO lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 16

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 Środki techniczne i organizacyjne

§ 17.

W celu ochrony danych spełniono wymogi, o których mowa w RODO, w szczególności:

a) przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach,
b) do przetwarzania danych zostali dopuszczeni wyłącznie pracownicy oraz osoby współpracujące ze Spółdzielnią na podstawie umów cywilnoprawnych upoważnione przez administratora danych zgodnie, które podpisały oświadczenia;
c) do przetwarzania danych zostali dopuszczeni wyłącznie członkowie Rady Nadzorczej Spółdzielni Budowlano-Mieszkaniowej ZACHÓD;
d) Osoby upoważnione do przetwarzania danych osobowych będą szkolone co najmniej raz w roku w zakresie ochrony danych osobowych.
e) zawarto umowy powierzenia przetwarzania danych;
f) została opracowana i wdrożona niniejsza Polityka.

§ 18.

W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:

a) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi zamykanymi na klucz bądź zamek elektroniczny (niewzmacnianymi, nieprzeciwpożarowymi);
b) zbiory danych osobowych przechowywane są w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej;
c) pomieszczenia, w którym przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy;
d) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, objęty jest systemem kontroli dostępu;
e) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych na klucz niemetalowych szafach;
f) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych na klucz metalowych szafach;
g) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej;
h) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej niemetalowej szafie;
i) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej metalowej szafie;
j) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej;
k) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy;
l) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 19.

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

a) zastosowano urządzenia typu UPS chroniący system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
b) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
c) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych;

d) zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł;
e) zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych;
f) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;
g) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
h) użyto system Firewall do ochrony dostępu do sieci komputerowej;
i) użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

§ 20.

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) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych;
f) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;

§ 21.

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 8 Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 22.

1. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza Zarząd we współpracy z Koordynatorem ds. ochrony danych osobowych oraz Zastępcą .
2. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
3. Na podstawie wyników przeprowadzonej analizy ryzyka, wskazani przez administratora danych właściciele procesów lub administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.
4. Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.

5. Administrator danych nie może zlekceważyć ryzyk, których wartość przekracza poziom minimalnego zagrożenia.

Rozdział 9 Procedura współpracy z podmiotami zewnętrznymi

§ 23.

1. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z wzorem stanowiącym **załącznik nr 13 do Polityki.**
2. Wzór wykazu podmiotów przetwarzających zawiera **załącznik nr 14 do Polityki.**
3. Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z RODO wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać.

Rozdział 10 Procedura domyślnej ochrony danych

§ 24.

1. Administrator danych 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 administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

Rozdział 11 Procedura zarządzania incydentami

§ 25.

1. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Administrator danych 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.
3. Administrator danych 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.
4. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych.
5. Zarząd we współpracy z Koordynatorem 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.**

Rozdział 12 Procedura realizacji praw osób

§ 26.

Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w RODO administrator danych rozpatruje indywidualnie.

§ 27.

Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

a) prawo dostępu do danych,
b) prawo do sprostowania danych,
c) prawo do usunięcia danych,

d) prawo do przenoszenia danych,
e) prawo do sprzeciwu wobec przetwarzania danych,
f) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.

§ 28.

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

§ 29.

Administrator danych 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 13 Procedura odbierania zgód oraz informowania osób

§ 30.

W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, zgodnie z **załącznikiem nr 17 do Polityki.**

§ 31.

W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych 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.**

§ 32.

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

Rozdział 14 Procedura użytkowania komputerów przenośnych i telefonów

§ 33.

1. Pracownicy upoważnieni do przetwarzania danych osobowych i pracujący na komputerach przenośnych i telefonach zobowiązani są do przestrzegania niniejszych zasad.
2. Dane osobowe lub danych poufne muszą zostać zaszyfrowane na dysku i zabezpieczone hasłem.
3. 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.
4. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie/problem administratorowi bezpieczeństwa informacji.
5. 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 zwykłej teczce, aktówce,
   2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej.

6. 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.
7. Użytkownik komputera i telefonu przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych
8. 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.

Rozdział 15
Postanowienia końcowe

§ 34.

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.

§ 35.

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 22 maja 2018 roku i obowiązuje od dnia jej przyjęcia.