Załącznik
do Uchwały Nr 3/04/2019
Zarządu SM „Skarbek” z dnia 17.05.2019 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Spółdzielni Mieszkaniowej „Skarbek” w Wałbrzychu

Oznaczenie użytych w niniejszej Polityce definicji:

1. *Administrator Danych Osobowych (ADO)* – Spółdzielnia Mieszkaniowa „Skarbek" w Wałbrzychu (dalej również jako: *„Spółdzielnia")*z siedzibą przy ul. S. Moniuszki 66I w Wałbrzychu (58-300), zarejestrowana pod numerem KRS 0000069409, podmiot przetwarzający dane osobowe.
2. *Administrator systemu informatycznego (ASI)* – informatyk posiadający upoważnienie od ADO do pełnienia funkcji Administratora systemu informatycznego.
3. *Dane osobowe* – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
4. *Przetwarzanie danych* – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
5. *RODO* – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz.Urz.UE L 119 z 4 maja 2016r.).
6. *Członkowie Spółdzielni* – osoby posiadające status członka Spółdzielni Mieszkaniowej „Skarbek" w Wałbrzychu.
7. *Osoby niebędące Członkami Spółdzielni* – właściciele, współwłaściciele bądź dzierżawcy lub najemcy lokali mieszkaniowych albo lokali użytkowych znajdujących się w zasobach Spółdzielni Mieszkaniowej „Skarbek" w Wałbrzychu oraz członkowie Wspólnot zarządzanych przez Spółdzielnię, nie posiadający statusu Członka Spółdzielni, a także spadkobiercy i pełnomocnicy wymienionych kategorii osób.
8. *Polityka bezpieczeństwa* – Polityka bezpieczeństwa danych osobowych w Spółdzielni.
9. *Przepisy krajowe* – ustawa z dnia 24 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz.1000) oraz inne regulacje krajowe służące stosowaniu 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 (Dz.Urz. UE L 119 z 4 maja 2016 r.).
10. *Instrukcja* – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Spółdzielni.
11. *System informatyczny* – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzana danych.
12. *System Internetowej Obsługi Kontrahenta* – serwis internetowy stanowiący zdalne narzędzie służące do wspomagania działalności Spółdzielni oraz ułatwienia kontaktów i przepływu informacji z poszczególnymi osobami posiadającymi tytuł prawny do lokalu znajdującego się w zasobach Spółdzielni.
13. *Użytkownik* – osoba upoważniona do przetwarzania danych osobowych w Spółdzielni.
14. *Wspólnoty* – wszystkie Wspólnoty mieszkaniowe, w których ADO sprawuje zarząd na podstawie art.18 ust.1 ustawy o własności lokali z dnia 24 czerwca 1994 r. (tj Dz.U z 2018r. poz.716).

I POSTANOWIENIA OGÓLNE

§1

1. Polityka bezpieczeństwa danych osobowych ma na celu wdrożenie i utrzymanie odpowiednich środków technicznych i organizacyjnych dla zapewnienia bezpieczeństwa danych osobowych i ich przetwarzania zgodnie z wymogami określonymi w Rozporządzeniu 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 (Dz.U. UE. L.2016. 119.1) oraz Ustawie z dnia 18 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018r. poz. 1000 z późn. zm.) i innych regulacji krajowych.

2. Realizując Politykę bezpieczeństwa i zarządzając danymi należy zapewnić ich:

a) poufność – dane nie są udostępniane lub ujawniane nieupoważnionym osobom, podmiotom,
b) integralność i przejrzystość – dane nie są zmieniane lub zniszczone w sposób nieautoryzowany a ich przetwarzanie wykonywane jest w sposób przejrzysty i zrozumiały dla osoby której dane dotyczą,
c) dostępność – możliwość wykorzystania ich na żądanie według określonych kryteriów pozwalających na łatwy dostęp do danych osobowych także ułatwiający osobom, których dane dotyczą wykonywanie praw przysługującym im na mocy art.15-22 RODO (dostęp, prawo sprostowania lub usunięcia). W przypadku konieczności udostępniania dokumentów i danych należy bezwzględnie stosować anonimizację tych danych osobowych wśród których znajdują się dane nie mające związku z celem udostępnienia,
d) rozliczalność – możliwość jednoznacznego przypisania działań konkretnym osobom.

3. Cele wyznaczone w Polityce bezpieczeństwa realizowane są poprzez:

a) udoskonalanie organizacyjnych i technicznych środków ochrony danych osobowych,
b) stosowanie odpowiednich urządzeń i programów do przetwarzania i zabezpieczania danych osobowych.

II CELE POLITYKI BEZPIECZEŃSTWA

§2

1. Wdrożenie Polityki bezpieczeństwa danych związane jest z maksymalnym ograniczeniem ryzyka nieuprawnionego przetwarzania lub utraty danych osobowych a w szczególności w celu ochrony interesów osób, których dane dotyczą i aby dane te były:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych),
d) przechowywanie w formie umożliwiającej identyfikację osoby, której dane dotyczą nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,

e) prawidłowe i w razie potrzeby uaktualnione (dane nieprawidłowe winne być niezwłocznie usunięte lub sprostowane).

2. Polityka bezpieczeństwa odnosi się do:

a) danych osobowych przetwarzanych przez Spółdzielnię w utworzonych zbiorach danych osobowych,

b) danych, które powierza się do przetwarzania innym podmiotom,

c) danych, których przetwarzanie zostało Spółdzielni powierzone na podstawie umów.

UZYSKIWANIE I WYKORZYSTANIE DANYCH OSOBOWYCH

§3

1. Dane osobowe przetwarzane w Spółdzielni mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą lub innych źródeł, w granicach dozwolonych przepisami prawa.

2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

3. W przypadku, gdy dane osobowe są niekompletne, nieprawdziwe lub nieaktualne albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

ZBIORY DANYCH OSOBOWYCH

§4

1. Zbiorem danych osobowych jest uporządkowany zestaw danych osobowych dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany czy rozproszony funkcjonalnie.

2. Dane osobowe gromadzone w zbiorach są przetwarzane w systemach informatycznych oraz w formie papierowej i są zlokalizowane w pomieszczeniach należących do obszaru przetwarzania danych osobowych określonych w załączniku nr 1 do niniejszej Polityki.

3. Wykaz zbiorów danych osobowych w Spółdzielni określa załącznik nr 2 do niniejszej Polityki.

4. Obszar przetwarzania danych osobowych, o którym mowa w ust.2 na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych jest zabezpieczony przed dostępem osób nieuprawnionych. Przebywanie osób nieuprawnionych do przetwarzania danych jest dopuszczalna za zgodą ADO lub w obecności osoby upoważnionej.

§5

1. W ramach prowadzonej przez Spółdzielnię działalności Spółdzielnia tworzy zbiór danych osobowych członków Spółdzielni do przetwarzania, których podstawą są przepisy ustawy z dnia 15 grudnia 2000r. o spółdzielniach mieszkaniowych (Dz.U.z 2018r. poz. 845 z późn.zm.), Prawa Spółdzielczego (tj.Dz.U. z 2018r. poz.1285), innych ustaw oraz Statutu Spółdzielni. Przetwarzanie danych członków odbywa się w oparciu art.6 ust.1 lit.c i f RODO.

2. W ramach prowadzonej przez Spółdzielnię działalności tj. zarządzania nieruchomościami Spółdzielnia tworzy zbiory danych osobowych:

a) właścicieli lokali w nieruchomościach stanowiących współwłasność Spółdzielni, w których wykonuje zarząd powierzony, o którym mowa w art.18 ust 1 ustawy z dnia 24 czerwca 1994 r. o własności lokali (zarządzanie powierzone odbywa się na podstawie art.27 ust.2 ustawy z dnia 15 grudnia 2000r. o spółdzielniach mieszkaniowych

b) właścicieli lokali w nieruchomościach będących Wspólnotami Mieszkaniowymi, zarządzanymi przez Spółdzielnię na podstawie zawartej umowy, działając w imieniu i na rzecz Wspólnoty Mieszkaniowej będącej administratorem danych osobowych członków wspólnoty,

c) najemców, dzierżawców lokali mieszkalnych i użytkowych znajdujących się w zasobach Spółdzielni.

3. W celu udokumentowania wszystkich procesów przetwarzania danych osobowych, Spółdzielnia Mieszkaniowa prowadzi rejestr czynności przetwarzania danych osobowych, o którym mowa w art.30 RODO, którego wzór stanowi załącznik nr 8 do niniejszej Polityki.

ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH (ADO)

§6

1. Administratorem Danych Osobowych w Spółdzielni jest Spółdzielnia reprezentowana przez Zarząd Spółdzielni (ADO) w skład którego wchodzą osoby uprawnione do reprezentacji Spółdzielni na podstawie odrębnych przepisów bądź osoba, której zadania ADO zostały powierzone.

2. Do obowiązków ADO należy:

a) wprowadzenie i stosowanie odpowiednich środków organizacyjnych i technicznych zapewniających ochronę danych osobowych odpowiednią do zagrożeń zapewniając ich poufność, integralność i rozliczalność,

b) informowanie użytkowników o obowiązkach wynikających z przepisów o ochronie danych osobowych RODO i Krajowych zwłaszcza w zakresie Polityki bezpieczeństwa oraz Instrukcji zarządzania Systemem Informatycznym i nadzór nad ich przestrzeganiem,

c) zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawniona, przetwarzaniem z naruszeniem Przepisów krajowych i RODO oraz zmianą, utratą, uszkodzeniem,

d) nadawanie, zmiana lub cofanie uprawnień do przetwarzania danych osobowych pracownikom i osobom zatrudnionym w Spółdzielni na podstawie umów cywilnoprawnych,

e) wystawianie upoważnień do przetwarzania danych osobowych, które powinny zawierać: imię i nazwisko osoby upoważnionej, datę nadania oraz zakres upoważnienia do przetwarzania danych osobowych,

f) odbierania oświadczeń o zachowaniu poufności,

g) nadzór nad stosowaniem środków technicznych i organizacyjnych zapewniających ochronę danych osobowych, w tym monitorowanie wdrożonych zabezpieczeń systemu informatycznego oraz nadzór nad oprogramowaniem systemu informatycznego,

h) nadzorowanie nad opracowaniem i aktualizowaniem dokumentacji dotyczącej przetwarzania danych osobowych wraz z wdrożeniem nowych rozwiązań w zakresie bezpieczeństwa przetwarzania danych,

i) nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,
j) nadzór nad prawidłowością archiwizacji dokumentów zawierających dane osobowe oraz zapewnienie nadzoru nad właściwym usuwaniem bądź niszczeniem dokumentów z danymi osobowymi,
k) analiza okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych,
l) prowadzenie i aktualizacja Rejestru czynności przetwarzania danych osobowych,
m) prowadzenie i aktualizacja Rejestru kategorii czynności przetwarzania danych osobowych dokonywanych przez Spółdzielnię w imieniu administratora danych,
n) informowanie osób, których dane osobowe są pozyskiwane przez Spółdzielnię

3. ADO wyznacza Administratora systemu informatycznego mającego wiedzę i umiejętności z obszaru ochrony danych osobowych oraz dającego rękojmię należytego wykonywania obowiązków Administratora systemu informatycznego, określonych w Polityce bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym, Instrukcji komputerowej ewidencji księgowej.

4. ADO prowadzi wszelkie ewidencje, wykazy i rejestry, o których mowa w Polityce bezpieczeństwa, Instrukcjach, przepisach, RODO oraz obowiązujących Przepisach krajowych, między innymi wykaz programów oraz przepływ informacji (zał. nr 3), wykaz zewnętrznych nośników informacji (zał. nr 9), wykazy obowiązujących druków (zał. nr 10).

ZADANIA (PRAWA I OBOWIĄZKI) ADMINSTRATORA SYSTEMU INFORMATYCZNEGO

§7

1. Administrator systemu informatycznego (ASI) odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Spółdzielni.

2. Do obowiązków Administratora systemu w zakresie ochrony danych osobowych należy w szczególności:

a) zapewnienie bezpiecznego wyłączenia serwerów na wypadek awarii i zabezpieczenie danych przed uszkodzeniem, Regulamin serwerowi stanowi zał. nr 6
b) dokonywanie przeglądu, napraw, konserwacji i likwidacji sprzętu komputerowego, na którym zapisane są dane osobowe, a w przypadku realizacji tych zadań przez podmiot zewnętrzny – nadzór nad realizacją w/w zadań,
c) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Spółdzielni w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych,
d) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
e) podejmowanie działań w przypadku naruszeń w systemie zabezpieczeń,
f) podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.

3. ASI doradza ADO przy podejmowaniu decyzji związanych z funkcjonowaniem systemów informatycznych, zapewnieniem odpowiedniego poziomu bezpieczeństwa oraz innych rozwiązań informatycznych, których wdrożenie zapewni lepszą wydajność pracy ze sprzętem informatycznym oraz większą ochronę przetwarzania danych osobowych.

4. ASI podejmuje inne działania, poza wymienionym w ust.1-3, zwłaszcza te, o których wspominają przepisy instrukcji lub które wynikają z charakteru sprawowanej funkcji.

ZADANIA I ODPOWIEDZIALNOŚĆ OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE (UŻYTKOWNIKÓW)

§8

1. Prawo do przetwarzania danych osobowych użytkownik otrzymuje na podstawie wydanego przez ADO upoważnienia określającego zakres przetwarzania danych z jednoczesnym przyjęciem oświadczenia użytkownika o obowiązkach określonych poniżej. Wzór upoważnienia stanowi załącznik nr 4 do niniejszej Polityki.

2. Każdy użytkownik ma obowiązek:

a) zapoznania się i stosowania obowiązujących przepisów z zakresu ochrony danych osobowych oraz wewnętrznych unormowań Spółdzielni w tym zakresie,

b) utrzymania właściwego poziomu bezpieczeństwa w zakresie swoich obowiązków i uprawnień,

c) zapewnienia poufności, integralności i rozliczalności danych osobowych,

d) zarówno w trakcie, jak i po ustaniu zatrudnienia w Spółdzielni chronić wszelkie informacje dotyczące funkcjonowania systemów i urządzeń służących do przetwarzania danych osobowych oraz sposobów zabezpieczenia danych,

e) przetwarzać dane osobowe tylko w zakresie wynikającym z jego obowiązków służbowych oraz zakresu określonego w wydanym Mu upoważnieniu,

f) zgłaszać ADO wszelkie zastrzeżenia co do bezpieczeństwa danych osobowych oraz wszelkie naruszenia bezpieczeństwa danych.

3. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Spółdzielni stanowi załącznik nr 7 do niniejszej Polityki.

4. Za przetwarzanie danych osobowych niezgodnie z prawem i celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których dane te dotyczą, grozi odpowiedzialność karna wynikająca z obowiązujących Przepisów krajowych lub odpowiedzialność pracownicza na zasadach określonych w Kodeksie pracy. Jednocześnie wobec osób, które nie stosują się do zapisów Polityki bezpieczeństwa, Instrukcji, RODO oraz obowiązujących Przepisów krajowych, ADO może wyciągnąć konsekwencje przewidziane w przepisach prawa pracy, zawartych w umowach cywilnoprawnych oraz w innych aktach prawnych w zależności od rodzaju skutków naruszeń.

DANE OSOBOWE W FORMIE PAPIEROWEJ

§9

1. Dokumenty zawierające dane osobowe kompletowane są w teczkach i segregatorach stanowiące dokumentację Spółdzielni z zachowaniem w szczególności zasady anonimizacji dokumentów:

a) powielanie dokumentacji w formie papierowej dokonuje osoba upoważniona i w takiej liczbie egzemplarzy jaka jest potrzebna do prawidłowego wykonania zadania,

b) dokumenty nie mogą być pozostawione poza miejscem pracy

c) teczki lub segregatory prowadzone są w uporządkowany sposób lub w zbiorze spraw danej osoby lub podmiotu, których dane dotyczą,

d) dokumenty zawierające dane osobowe przekazywane są bezpośrednio do rąk własnych użytkowników.

2. Dokumenty zawierające dane osobowe przechowywane są w szafach zamykanych na klucze, znajdujące się w pomieszczeniach wskazanych jako miejsca przetwarzania danych osobowych, ujęte w załączniku nr 1 do niniejszej Polityki, stosując politykę kluczy i dostępu do pomieszczeń określoną w zał. nr 5

3. Wszelkie dokumenty zawierające dane osobowe, po ustaniu ich codziennej przydatności podlegają archiwizacji, a w momencie ustania podstawy ich przetwarzania podlegają zniszczeniu przy użyciu niszczarki zapewniającej odpowiedni poziom tajności. Odpowiednia niszczarka znajduje się w jednym z pomieszczeń biurowych.

4. Dokumenty zawierające w swojej treści dane osobowe archiwizowane są w składnicy akt, zgodnie z Regulaminem archiwizowania akt i funkcjonowania składnicy akt w Spółdzielni.

5. Raz w roku ADO dokonuje weryfikacji teczek, w wyniku której podejmuje decyzję o przekazaniu dokumentów do zniszczenia. Zniszczenie dokumentów odbywa się częściowo w siedzibie Spółdzielni i dokonywane jest przez upoważnione przez ADO osoby. W przypadku zgromadzenia większej liczby dokumentów przeznaczonych do zniszczenia, Spółdzielnia nawiązuje w tym celu współpracę z firmą zewnętrzną, po uprzednim podpisaniu umowy w zakresie powierzenia danych osobowych do zniszczenia.

DANE OSOBOWE W FORMIE ELEKTRONICZNEJ

§10

1. Postępowanie z danymi osobowymi w formie elektronicznej odbywa się na zasadach określonych w niniejszej polityce bezpieczeństwa danych, a także zgodnie z przepisami Instrukcji zarządzania Systemem Informatycznym, Instrukcji Komputerowej ewidencji Księgowej i innych wewnętrznych unormowaniach.

2. Użytkownik uzyskuje dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, poprzez zalogowanie się na indywidualne konta przy użyciu loginu oraz hasła dostępu nadanego przez Administratora systemu na zlecenie ADO, na zasadach określonych w instrukcji.

3. ADO ma dostęp do wszystkich loginów i haseł stosowanych przez pracowników obsługujących systemy informatyczne.

4. Użytkownik w czasie korzystania z systemu informatycznego używa baz danych w programach, które zostały udostępnione przez ADO stosownie do charakteru wykonywanych obowiązków i wydanego upoważnienia.

5. Niedozwolone jest przekazywanie plików przy użyciu sieci Internet poza obszar przetwarzania danych osobowych wskazany w niniejszej Polityce bezpieczeństwa. Wyjątkiem od powyższego zakazu jest przesłanie dokumentu członkowi Spółdzielni, kontrahentowi lub innemu pracownikowi Spółdzielni drogą mailową, przy użyciu służbowej skrzynki mailowej.

6. Użytkownik w ramach nadanych mu uprawnień korzysta z programów za pośrednictwem których przetwarzane są dane osobowe w tworzonych przez Spółdzielnię zbiorach danych tj. członków Spółdzielni, osób niebędących członkami Spółdzielni, pracowników, kontrahentów, osób zatrudnionych na podstawie umów cywilnoprawnych.

7. Niedozwolone jest jakiekolwiek kopiowanie i utrwalanie przetwarzanych w systemach informatycznych danych osobowych.
8. Po zakończeniu pracy, Użytkownik zobowiązany jest do zapisania otwartych plików, a następnie wylogowania ze wszystkich kont w systemie informatycznym.

INSTRUKCJA POSTEPOWANIA NA OKOLICZNOŚĆ NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§11

1. W procesach przetwarzania danych osobowych do naruszenia ich praw i wolności może dochodzić w wyniku:
a) niewłaściwego (niezgodnego z celem) ich wykorzystania,
b) niewłaściwego ich zabezpieczenia przed dostępem osób nieuprawnionych,
c) nieodpowiedniego zarządzania uprawnieniami do ich przetwarzania,
d) wszelkiego rodzaju zdarzeń losowych lub celowych (nieuprawnione ujawnienie, zniszczenie, utrata lub ich modyfikacja.
2. Naruszenie ochrony danych osobowych oznacza 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.
3. W przypadku stwierdzenia naruszenia ochrony danych osobowych przetwarzanych w zbiorach danych lub naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych a także podejrzenia naruszenia danych ze względu na stan urządzenia, zawartość zbioru danych – każdy użytkownik jest zobowiązany do:
a) niezwłocznego powiadomienia o tym ADO,
b) podjęcia czynności niezbędnych do powstrzymania skutków naruszenia ochrony, ustalenia przyczyny i sprawcy naruszenia ochrony.
4. W przypadku stwierdzenia naruszenia ochrony danych lub naruszenia zabezpieczenia systemu informatycznego należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia bezpośredniego przełożonego, Administratora systemu informatycznego, osoby działającej w imieniu ADO.
5. Każda sytuacja naruszenia ochrony danych lub naruszenia zabezpieczenia systemu informatycznego niezwłocznie odnotowywana jest w rejestrze incydentów zagrażających bezpieczeństwu danych osobowych.
6. Rejestr incydentów, o którym mowa w ust.6, prowadzony jest przez ADO, przy udziale Administratora systemu.
7. W rejestrze incydentów, o którym mowa w ust.6, odnotowuje się w szczególności:

a) imię i nazwisko Użytkownika zgłaszającego incydent,
b) datę zgłoszenia incydentu,
c) datę i przybliżony czas wystąpienia incydentu,
d) opis zaistniałego incydentu, uwzględniający w szczególności, czy dotyczył on danych przetwarzanych w formie papierowej, czy z zastosowaniem systemu informatycznego,
e) charakter naruszenia danych osobowych w tym – w miarę możliwości – kategorie i przybliżoną liczbę osób, których dane dotyczą a także kategorie i przybliżoną liczbę wpisów danych osobowych,
f) opis czynności podjętych w celu rozwiązania problemu stanowiącego incydent,

g) datę i przybliżony czas zakończenia czynności, o których mowa w li.f)
h) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
i) ocenę czy naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
j) opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w szczególności w celu Zminimalizowania jego ewentualnych negatywnych skutków.

8. Oceny, czy naruszenie skutkowało ryzykiem naruszenia pracy lub wolności osób fizycznych o których mowa w ust.8 lit.i), dokonuje ADO przy udziale Administratora systemu. W szczególności ocena ta dotyczy, czy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o których mowa w art.34 ust.1 RODO.

9. ADO wraz z Administratorem systemu ustala niezbędność, charakter oraz zakres zastosowania środków o których mowa w ust.8 lit.j). ADO podejmuje decyzję w sprawie wdrożenia takich środków.

10. W przypadku naruszenia ochrony danych osobowych ADO zgodnie z art. 33 ust.1 RODO zgłasza ten fakt organowi nadzorczemu, chyba że wykaże małe prawdopodobieństwo by to naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

INFORMOWANIE OSÓB, KTÓRYCH DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

1. W trybie art.34 RODO , w przypadku naruszenia ochrony danych osobowych w Spółdzielni powodującym wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą ADO bez zbędnej zwłoki zawiadamia, z wyjątkiem wystąpienia jednej z poniższych przesłanek:
a) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności, szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
b) ADO zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

2. Zawiadomienie winno opisywać charakter naruszenia ochrony danych osobowych osoby, której dane dotyczą, a także:
a) dane kontaktowe osoby, która może udzielić wszelkich informacji związanej z naruszeniem danych,
b) opis możliwych konsekwencji naruszenia ochrony danych (np. kradzież lub sfałszowanie tożsamości, strata finansowa, naruszenie dobrego imienia),
c) opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych w tym też środki w celu zminimalizowania jego ewentualnie negatywnych skutków.

§12

OCENA SKUTKÓW DLA OCHRONY DANYCH

1. Administrator dokonuje analizę i ocenę skutków dla ochrony danych oraz ustala, czy przetwarzanie danych może powodować (z dużym prawdopodobieństwem) wysokie

ryzyko naruszenia praw lub wolności osób fizycznych o których mowa w art.35 ust. 1 RODO.

2. Dostosowanie środków ochrony przetwarzania danych osobowych do skali ryzyka winno opierać się na ocenie ich pod kątem utraty poufności, integralności i dostępności danych, biorąc przy tym pod uwagę ich zakres, szczególne znaczenie oraz kontekst i cele przetwarzania a tym samym również kwestie zapewnienia bezpieczeństwa przetwarzania, autentyczności i rozliczalności danych.

3. Dokumentacja, o której mowa w ust.1 winna składać się w szczególności z:

a) analizy, czy dany rodzaj przetwarzania danych osobowych ze względu na swój charakter, zakres, kontekst i cele może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych,

b) wykaz rodzajów operacji przetwarzania, dla których ocena skutków przetwarzania wynika z przepisów prawa,

c) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania w tym gdy ma to zastosowanie w przypadkach, prawnie uzasadnionych interesów realizowanych przez ADO,

d) ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,

e) ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą,

f) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie zapisów RODO.

4. Przy przygotowywaniu lub aktualizowaniu dokumentacji o której mowa w ust.1, ADO w stosownych przypadkach zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.

§13

POSTANOWIENIA KOŃCOWE

1. Integralną część Polityki bezpieczeństwa stanowią następujące załączniki:

- Załącznik nr 1 – „Wykaz miejsc przetwarzania danych osobowych”
- Załącznik nr 2 – „Wykaz zbiorów danych osobowych i opis struktury tych danych”
- Załącznik nr 3 – „Wykaz programów oraz przepływy informacji”
- Załącznik nr 4 – „Wzór upoważnienia do przetwarzania danych osobowych dla pracowników wraz z oświadczeniem o zachowaniu poufności”
- Załącznik nr 5 – „Polityka kluczy i dostępu do pomieszczeń w Spółdzielni Mieszkaniowej „Skarbek” w Wałbrzychu”
- Załącznik nr 6 – „Regulamin serwerowni w Spółdzielni Mieszkaniowej „Skarbek”
- Załącznik nr 7 – „Ewidencja osób upoważnionych do przetwarzania danych osobowych w Spółdzielni Mieszkaniowej „Skarbek” w Wałbrzychu”
- Załącznik nr 8 – „Wzór rejestru czynności przetwarzania danych osobowych”
- Załącznik nr 9 – „ Wykaz zewnętrznych nośników informatycznych „
- Załącznik nr 10 – „Wykaz obowiązujących druków”

2. Niniejsza Polityka bezpieczeństwa danych osobowych w celu jej stosowania przekazana zostanie w formie elektronicznej pracownikom Spółdzielni, upoważnionym do przetwarzania danych osobowych a wersja w formie papierowej – podpisana przez Zarząd Spółdzielni znajdować się będzie w Dziale Organizacyjnym.

3. Niniejsza Polityka bezpieczeństwa wchodzi w życie z dniem 17.05.2019 r. tj. z chwilą podjęcia uchwały Zarządu o jej wprowadzeniu.

Zarząd SM „Skarbek”