Załącznik Nr 1

Do Uchwały Zarządu nr 1/2016

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH w SPÓŁDZIELNI MIESZKANIOWEJ „ODRODZENIE” w Kożuchowie

Deklaracje

§ 1

Zarząd Spółdzielni Mieszkaniowej „Odrodzenie" w Kożuchowie świadom wagi problemów związanych z ochroną danych osobowych przetwarzanych w Spółdzielni w związku z wykonywaniem ustawowych i statutowych obowiązków deklaruje:

1. zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,
2. zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w spółdzielni w zakresie problematyki i bezpieczeństwa tych danych,
3. zamiar traktowania obowiązków osób przetwarzających dane osobowe jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania,
4. zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych,
5. stale doskonalić i rozwijać organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie, tak, aby skutecznie zapobiegać zagrożeniom.

Definicje

§ 2

1. Administrator Danych (zwany dalej AD) - Spółdzielnia Mieszkaniowa „Odrodzenie" w Kożuchowie z siedzibą przy ul. 22 Lipca 12C
2. Administrator Bezpieczeństwa Informacji (zwany dalej ABI)- osoba nadzorująca przestrzeganie zasad bezpieczeństwa danych osobowych, wyznaczonych przez AD
3. Administrator Systemów Informatycznych (zwany dalej ASI) - osoba odpowiedzialna za wdrożenie i stosowanie zasad bezpieczeństwa systemów informatycznych, zobowiązana do stosowania technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych wyznaczonych przez AD
4. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby. 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.
5. System Informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
6. Zbiór danych osobowych – posiadający strukturę - zestaw danych o charakterze osobowym.

Cel polityki bezpieczeństwa danych osobowych

§ 3

1. Celem niniejszej polityki jest określenie kierunków działań dla zapewnienia bezpieczeństwa danych osobowych przetwarzanych przez Spółdzielnię. Przez bezpieczeństwo przetwarzania danych należy rozumieć:
   - poufność – zapewnienie, że dane są dostępne jedynie osobom upoważnionym
   - integralność- zapewnienie dokładności i kompletności danych oraz metod przetwarzania,
   - dostępność- zapewnienie, że osoby upoważnione mają dostęp do danych i związanych z nimi

aktywów wtedy, gdy jest to potrzebne,
- rozliczalność - zapewnienie, że działania osób można jednoznacznie przypisać tym osobom.

2. Dane osobowe w spółdzielni przetwarzane są dla zabezpieczenia prawidłowej realizacji zadań, w szczególności:
   - wynikających z ustawy z dnia 16 września 1982r. Prawo Spółdzielcze (tekst pierwotny Dz.U.1982r.Nr30 poz210 z późn.zm.)zwana dalej ps,
   - wynikających z ustawy z 15 grudnia 2000r o spółdzielniach mieszkaniowych ???(tekst pierwotny:Dz.U.2001r.Nr 4 poz.27 z późn.zm.)zwana dalej usm,
   - wynikających z ustawy z dnia 24 czerwca 1994r o własności lokali (tekst pierwotny:Dz.U.1996r Nr 85 poz388 z późn.zm zwana dalej uwl,
   - wynikających ze statutu spółdzielni i regulaminów,
   - w celu zapewnienia prawidłowej, zgodnej z prawem i celami spółdzielni polityki personalnej oraz bieżącej obsługi stosunków pracy a także innych stosunków cywilno prawnych nawiązywanych przez Spółdzielnię, działającą jako pracodawca w rozumieniu art.3 kodeksu pracy lub strona innych stosunków cywilnoprawnych.
3. Spółdzielnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   - przetwarzane zgodnie z prawem,
   - zbieranie 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 identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
4. Spółdzielnia jako AD zarządza bezpieczeństwem danych osobowych je określony przez:
   - Politykę bezpieczeństwa danych osobowych Spółdzielni Mieszkaniowej „Odrodzenie" w Kożuchowie,
   - Instrukcję zarządzania systemem informatycznym w Spółdzielni Mieszkaniowej „Odrodzenie" w Kożuchowie,

Zakres stosowania

§ 4

Zakres stosowania niniejszego dokumentu obejmuje wszystkie dane osobowe przetwarzane w Spółdzielni, zarówno w formie elektronicznej jak i papierowej. Polityka obejmuje wszystkie osoby przetwarzające dane osobowe w spółdzielni.

Przetwarzanie danych osobowych

§ 5

1. Nadzór nad przestrzeganiem zasad ochrony danych osobowych w Spółdzielni wykonuje ABI.
2. ABI wyznacza Zarząd Spółdzielni i zgłasza do GIODO.
3. ASI w Spółdzielni jest firma UNISOFT obsługująca zintegrowany system informatyczny na podstawie zawartej umowy z Zarządem Spółdzielni.
4. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dopuszcza się do ich przetwarzania w systemie informatycznym lub tradycyjnym wyłącznie osoby posiadające upoważnienie nadane przez AD.
5. Zakres upoważnienia może wynikać w szczególności z charakteru pracy i z zakresu obowiązków wykonywanych na danym stanowisku pracy.

6. Dostęp do danych i ich przetwarzania bez odrębnego upoważnienia AD lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonych kategorii.
7. Polityka bezpieczeństwa w zakresie ochrony danych osobowych zapewnia kontrolę nad dostępem do tych danych.
8. Osoby nie przetwarzające danych osobowych określonej kategorii w związku z zatrudnieniem mające interes prawny i podstawę prawną w uzyskaniu dostępu do tych danych, mogą mieć do nich wgląd wyłącznie w obecności upoważnionego pracownika Spółdzielni.
9. Spółdzielnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia zaznajomienie osób upoważnionych do dostępu lub przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi a także środkami ochrony tych danych, stosowanymi w Spółdzielni.
10. Zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także środkami ochrony tych danych stosowanymi w Spółdzielni może odbywać się w szczególności poprzez:
    - Instruktaż na stanowisku pracy,
    - Szkolenie wewnętrzne realizowane przez Spółdzielnię,
    - Szkolenie zewnętrzne,
11. Osoby upoważnione przez AD do przetwarzania danych osobowych zostają zaznajomione o powinności zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia stosowanych w Spółdzielni.
12. Dane osobowe przetwarzane są w siedzibie Spółdzielni adres: ul. 22 Lipca 12C; 67-120 Kożuchów

Odpowiedzialność

§ 6

1. AD odpowiada za zabezpieczenie danych osobowych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, utratą, uszkodzeniem, zniszczeniem lub nieautoryzowaną zmianą.
2. W imieniu AD nadzór nad przestrzeganiem zasad ochrony danych osobowych sprawuje Administrator Bezpieczeństwa Informacji.
3. ABI jest zobowiązany do:
    - prowadzenia i aktualizacji ewidencji wydanych upoważnień do przetwarzania danych,
    - nadzorowania fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe, w szczególności systemu kontroli dostępu oraz kontroli przebywających w nich osób pod kątem posiadania upoważnienia do przetwarzania danych osobowych,
    - nadzorowania przestrzegania zasad określonych w polityce i instrukcjach dotyczących bezpieczeństwa danych osobowych,
    - nadzorowania obiegu oraz przechowywania dokumentów zawierających dane osobowe, w tym generowanych przez systemy informatyczne,
    - analizy sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych (jeśli takie wystąpiło) oraz przygotowania i przedstawienia AD propozycji zmian, które pozwolą uniknąć podobnych sytuacji w przyszłości,
    - szkolenia pracowników z zakresu bezpieczeństwa przetwarzania danych osobowych,
    - nadzorowania wycofania uprawnień dostępu do systemów informatycznych w przypadku odebrania pracownikowi upoważnienia do przetwarzania danych osobowych.
4. W celu realizacji powierzonych zadań Administrator Bezpieczeństwa Informacji ma prawo:
    - kontrolować wraz z ASI pracowników w zakresie właściwego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe oraz zabezpieczenia systemów informatycznych,

- wydawać polecenia pracownikom w zakresie bezpieczeństwa danych osobowych,
- informować AD o przypadkach naruszenia bezpieczeństwa danych osobowych,
- żądać od wszystkich pracowników wyjaśnień w sytuacjach podejrzenia naruszenia bezpieczeństwa danych osobowych.

5. Za techniczne aspekty funkcjonowania systemów informatycznych odpowiedzialny jest ASI.
6. ABI obowiązany jest do:
   - niezwłocznego wystąpienia do AD o przydzielenie uprawnień oraz wydanie upoważnienia do przetwarzania danych osobowych dla pracowników,
   - niezwłocznego wystąpienia do ASI o odebranie lub modyfikacje uprawnień dostępu do systemu informatycznego pracownikowi upoważnionemu do przetwarzania za jego pomocą danych osobowych w przypadku utraty przez pracownika upoważnienia w sytuacji: ustania stosunku pracy, zmiany stanowiska, komórki organizacyjnej, oddelegowania i innych,
7. Pracownicy Spółdzielni mają obowiązek poinformowania AD, za pośrednictwem ABI, o zamiarze utworzenia, likwidacji, modyfikacji struktury zbioru lub zmiany lokalizacji zbioru.
8. Każdy pracownik przetwarzający dane osobowe posiada upoważnienie do przetwarzania danych osobowych zawierające:
   - imię i nazwisko,
   - datę nadania i okres jego obowiązywania,
   - zakres danych, które osoba może przetwarzać (zbiory danych)
   - cel przetwarzania danych osobowych,
   - identyfikator użytkownika (dotyczy wyłącznie zbiorów danych prowadzonych w formie elektronicznej)
9. Każdy pracownik przetwarzający dane osobowe zobowiązany jest zapewnić ich należytą ochronę.

Wykaz i rejestr zbiorów danych osobowych

§ 7

1. Wykaz zbiorów danych osobowych wraz z opisem obszaru przetwarzania i struktury zbiorów danych prowadzi ABI.
2. Rejestr zbiorów danych osobowych prowadzi ABI zgodnie z art.36 ust.2pkt 2 i Rozporządzeniem Ministra Administracji i cyfryzacji w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbioru danych.
3. Wykaz określony w ust.1 i Rejestr określony w ust.2 stanowi część integralną Polityki bezpieczeństwa.

System zabezpieczeń danych osobowych

§ 8

1. Ochrona danych osobowych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nie uprawnioną modyfikacją lub usunięciem.
2. W celu ochrony danych przetwarzanych w systemie informatycznym należy wykorzystywać wchodzące w jego skład mechanizmy zarówno sprzętowe, jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo danych.
3. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, wiąże się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych.
4. W razie nieobecności pracownika upoważnionego do przetwarzania danych osobowych obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym, uniemożliwiającym dostęp do danych osobowych osobom niepowołanym.

5. Budynki, w których przetwarzane są zbiory danych osobowych są nadzorowane przez system kontroli alarmowej przez całą dobę.
6. Procedurę zarządzania uprawnieniami do systemów informatycznych reguluje „Instrukcja zarządzania systemem Informatycznym w Spółdzielni Mieszkaniowej „Odrodzenie".
7. Udostępnienie danych osobowych wymaga uzyskania zgody ABII.
8. Nowo przyjmowani pracownicy, którzy w ramach swoich obowiązków będą przetwarzali dane osobowe, zapoznają się z przepisami z zakresu danych osobowych oraz uregulowaniami wewnętrznymi Spółdzielni.
9. Pracownicy Spółdzielni są szkoleni z zakresu ochrony danych osobowych. Szkolenie obejmuje w szczególności treść ustawy o ochrony danych osobowych oraz zakres wewnętrznych uregulowań.

Konsekwencje naruszania Polityki bezpieczeństwa

§ 9

1. Naruszanie przez zatrudnione w ramach stosunku pracy osoby upoważnione do dostępu lub przetwarzania, może zostać potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie.
2. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia oraz znajdujących się w nim zbiorów danych jest niedopuszczalne i może zostać potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

Przeglądy i aktualizacje polityki bezpieczeństwa

§ 10

1. System bezpieczeństwa danych osobowych podlega corocznemu przeglądowi pod kątem aktualności i stosowalności. Przeglądu dokonuje zespół powołany przez Prezesa Spółdzielni. W skład zespołu wchodzi ABI.
2. Polityka bezpieczeństwa podlega aktualizacji każdorazowo w przypadku:
   - ~ likwidacji, utworzenia lub zmiany zawartości zbioru,
   - ~ zmiany lokalizacji zbioru,
   - ~ zmiany przepisów prawa dotyczących ochrony danych osobowych, wymagającej aktualizacji Polityki bezpieczeństwa
   - ~ innych znaczących zmian w funkcjonowaniu Spółdzielni, dotyczących danych osobowych
3. Projekt aktualizacji polityki przygotowuje ABI.

Załącznik Nr 2
Do Uchwały Zarządu Nr 1/2016

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z §3 ust.1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024).

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych. Upoważnienie nadaje i odwołuje administrator danych. Upoważnienie i jego odwołanie sporządzane są na piśmie, w dwóch jednobrzmiących egzemplarzach – jeden przeznaczony jest dla osoby, której nadano lub odebrano upoważnienie, drugi – dla administratora danych. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do Instrukcji. Wzór odwołania upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 2 do Instrukcji. Upoważnienia nie sporządza się dla administratora danych. Upoważnienia nadane przed dniem wprowadzenia Instrukcji pozostają w mocy.

Upoważnienia do przetwarzania danych osobowych rejestrowane są w rejestrze osób upoważnionych do przetwarzania danych osobowych. Wzór rejestru stanowi załącznik nr 3 do Instrukcji. Rejestr prowadzi administrator danych.

2. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem. W Spółdzielni Mieszkaniowej „Odrodzenie" w Kożuchowie obowiązują następujące zasady tworzenia hasła:

- hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,
- hasło musi składać się z co najmniej 6 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
- hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
- hasło nie może być jednakowe z identyfikatorem użytkownika,
- hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.

Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.

Hasło musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.

W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie administratora danych.

Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych

Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić administratora danych.

Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.

Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych

płyty CD, pendrive i inne, zawierają cych dane osobowe. Zakoń czenie pracy w systemie informatycznym służ ą cym do przetwarzania danych osobowych nastę pują poprzez wylogowanie się z tego systemu.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzę dzi programowych służ ą cych do ich przetwarzania

Za sporzą dzanie kopii zapasowych zbiorów danych odpowiedzialny jest uż ytkownik systemu informatycznego służ ą cego do przetwarzania danych osobowych.

Kopie awaryjne moż e tworzyć jedynie administrator danych. Kopie zapasowe powinny być kontrolowane przez administratora danych, w szczególnoś ci pod ką tem prawidłowoś ci ich wykonania poprzez czę ś ciowe lub całkowite odtworzenie na wydzielonym sprzę cie komputerowym.

Noś niki informatyczne zawierają ce dane osobowe lub kopie systemów informatycznych służ ą cych do przetwarzania danych osobowych są przechowywane w sposób uniemoż liwiają cy ich utratę , uszkodzenie lub dostę p osób nieuprawnionych.

W przypadku likwidacji noś ników informatycznych zawierają cych dane osobowe lub kopie zapasowe systemów informatycznych służ ą cych do przetwarzania danych osobowych należ y przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemoż liwiają cy odczyt danych osobowych.

5. Sposób, miejsce i okres przechowywania elektronicznych noś ników informacji zawierają cych dane osobowe oraz kopii zapasowych

Nie należ y przechowywać zbę dnych noś ników informacji zawierają cych dane osobowe oraz kopii zapasowych, a takż e wydruków i innych dokumentów zawierają cych dane osobowe. Po upływie okresu ich uż yteczno ś ci lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było moż liwe ich odczytanie.

Elektroniczne noś niki informacji zawierają ce dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowią ce obszar przetwarzania danych osobowych, okreś lony w „Polityce bezpieczeń stwa danych osobowych".

Elektroniczne noś niki informacji zawierają ce dane osobowe oraz kopie zapasowe, a takż e wydruki i inne dokumenty zawierają ce dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowią cych obszar przetwarzania danych osobowych, okreś lony w „Polityce bezpieczeń stwa danych osobowych", w sposób zabezpieczają cy je przed nieuprawnionym przejęciem, modyfikacją , uszkodzeniem i zniszczeniem.

W przypadku uszkodzenia lub zuż ycia noś nika informacji zwierają cych dane osobowe należ y go fizycznie zniszczyć tak, aby nie było moż liwe odczytanie danych osobowych.

6. Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.

Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym.

Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowanie oprogramowanie antywirusowe. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

7. Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

W systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, administrator danych odnotowuje je w rejestrze odbiorców danych osobowych. W rejestrze odnotowywane są imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. Wzór rejestru stanowi załącznik nr 4 do Instrukcji.

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w „Polityce bezpieczeństwa danych osobowych" przez firmy zewnętrzne na podstawie zawartych umów. W umowie musi znajdować się zapis o powierzeniu danych osobowych.

W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub

skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora danych.

Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.

Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni administrator danych. Administrator danych prowadzi dokumentację potwierdzającą wykonanie napraw, przeglądów i konserwacji, (załącznik nr 5 do Instrukcji)

Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez pracownika Spółdzielni Mieszkaniowej „Odrodzenie" w Koż uchowie.

9. Pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych.

Administrator danych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.

Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.