POLITYKA BEZPIECZEŃSTWA

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SPÓŁDZIELNIA MIESZKANIOWA W JANOWCU WIELKOPOLSKIM

GNIEŹNIEŃSKA 12/2, 88-430 JANOWIEC WIELKOPOLSKI

Data i miejsce sporządzenia dokumentu:	Janowiec Wielkopolski 30.06.2015 Aktualizacja 15.06.2018
Ilość stron:	31

SPIS TREŚCI

1. WSTĘP

1.1. INFORMACJE OGÓLNE

1. Administrator Danych, który wdraża Politykę Bezpieczeństwa.

Spółdzielnia Mieszkaniowa w Janowcu Wielkopolskim z siedzibą w Janowcu Wielkopolskim ul. Gnieźnieńska 12/2.

2. Celu wprowadzania dokumentu.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

3. Podstawy prawne.

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883),
- Rozporządzenie 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. 2004 nr 100 poz. 1024),
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015 nr 0 poz. 719),
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. 2015 nr 0 poz. 745),
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000),
- 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) dalej RODO.

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Na Politykę Bezpieczeństwa składają się następujące informacje:

1) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

4) sposób przepływu danych pomiędzy poszczególnymi systemami, określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1. **ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000), zwana dalej „Ustawą",
2. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. **przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
4. **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
5. **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalanie tożsamości osoby, której dane dotyczą
6. **systemie informatycznym** – rozumie się przez to system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informację
7. **systemie tradycyjnym** – rozumie się przez to zespól procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze,
8. **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada **Administrator danych osobowych**. Kierownik jednostki, kierownicy komórek organizacyjnych, pracownicy samodzielni obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą uszkodzeniem lub zniszczeniem.

2. **Administrator Bezpieczeństwa Informacji / Inspektor Ochrony Danych Osobowych** wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi. Szczegółowy zakres odpowiedzialności i obowiązków ABI:
   - nadzoruje bezpieczeństwo systemów informatycznych tradycyjnych,
   - nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących
   - procedur
   - doradza użytkownikom w zakresie bezpieczeństwa,
   - zapewnia, aby pracownicy posiadający dostęp do systemu informatycznego posiadali
   - nadane pisemne upoważnienie do przetwarzania danych osobowych,
   - prowadzi kontrole w zakresie bezpieczeństwa,
   - prowadzi ewidencje osób, którym nadano upoważnienie do przetwarzania danych
   - osobowych,
   - przygotowuje wnioski pokontrolne dla administratora danych osobowych.

3. **Administrator systemu informatycznego** wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzaniu systemem informatycznym, a w szczególności:
   - odpowiada za bezpieczeństwo systemu informatycznego,
   - zobowiązuje i bieżąco kontroluje stosowanie się użytkowników do obowiązujących
   - procedur,
   - utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu informatycznego,
   - zapewnia aktualizacje dokumentacji technicznej systemu, tym opis struktury zbiorów i ich
   - zależności
   - prowadzi ewidencje osób, którym nadano upoważnienie do przetwarzania danych

- osobowych,
- prowadzi wykaz pomieszczeń, w których przetwarzane są dane osobowe,
- prowadzi wykaz podmiotów, którym udostępniono dane osobowe,
- prowadzi wykaz podmiotów, którym powierzono dane osobowe do przetwarzania,
- prowadzi wykaz zbioru danych osobowych

4. **Osoby upoważnione do przetwarzania danych osobowych** mają obowiązek:
   - przetwarzać je zgodnie z przepisami,
   - nie udostępniać ich oraz uniemożliwić dostęp do nich osobom nieupoważnionym,
   - zabezpieczać je przed zniszczeniem

5. **Użytkownik systemu informatycznego** wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji bezpieczeństwa w szczególność do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważnienie do przetwarzania danych osobowych nadaje Administrator Bezpieczeństwa Informacji / Inspektor Ochrony Danych Osobowych na wniosek Administrator Danych w osobie Kierownika jednostki w formie pisemnej.
2. Indywidualny identyfikator w systemie informatycznym nadaje Administrator Systemu Informatycznego na wniosek Administrator Danych w osobie Kierownika jednostki.
3. Zakres nadanych uprawnień ustalany jest zgodnie ze stanowiskiem służbowym. Zakres przetwarzanych danych będzie wystarczający do wypełniania powierzonych obowiązków.
4. Rejestr upoważnień oraz rejestr Indywidualnych identyfikatorów w systemie informatycznym prowadzi Administrator Bezpieczeństwa Informacji / Inspektor Ochrony Danych Osobowych w formie pisemnej.

4. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

- Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
- Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
- W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
- Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
- Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
- Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
- Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

5. INSTRUKCJA POSTĘPOWNIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

- Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Systemów Informatycznych bądź Administratorowi Danych osobowych / Inspektorowi Ochrony Danych Osobowych.
- Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Systemów Informatycznych lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:
  - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
  - zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
  - udokumentować wstępnie zaistniałe naruszenie,
  - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Systemów Informatycznych lub osoby upoważnionej.
- Po przybyciu na miejsce naruszenia ochrony danych osobowych, Administrator Systemów Informatycznych lub osoba go zastępująca:
  - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania
  - wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- Administrator Systemów Informatycznych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport według wzoru stanowiącego Załącznik nr 2 do niniejszej Instrukcji. Raport, o którym mowa powyżej Administrator Systemów Informatycznych niezwłocznie przekazuje Administratorowi Bezpieczeństwa Informacji, a w przypadku jego nieobecności osobie wyznaczonej.
- Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Systemów Informatycznych zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

6. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

- Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim sprawuje Administrator Bezpieczeństwa Informacji / Inspektor Ochrony Danych Osobowych oraz Administrator Systemów Informatycznych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
- Czynności kontrolne przeprowadzane są na wniosek Kierownika Jednostki.
- Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności.
- Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji przechowywanej u Administratora Bezpieczeństwa Informacji.
- Wzór protokołu z kontroli lub czynności sprawdzających, o których mowa w niniejszym Rozdziale stanowi Załącznik nr 10 do niniejszej Polityki.

7. OPIS STRUKTURY ZBIORÓW DANYCH

Opis struktury zbiorów danych zawiera załącznik nr 6 do Polityki Bezpieczeństwa.

8. SPOSÓB PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

1. Przepływa danych następuje pomiędzy systemami:
    a. Księgowość SM/WM ProVirtus -> System Jednolitego Pliku Kontrolnego Ministerstwa Finansów
        i. Przekazywane są dane kontrahentów w postaci numeru NIP lub PESEL
        ii. Przekazywanie na podstawie wymogów prawa
    b. Program Płatnik -> System Zakładu Ubezpieczeń Społecznych
        i. Przekazywane są dane osobowe pracowników i współpracowników oraz członków rodzin w postaci Imię, Nazwisko, numer Dowodu Osobistego, numer PESEL, adres zamieszkania
        ii. Przekazywanie na podstawie wymogów prawa

9. OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

- Dane osobowe przetwarzane i przechowywane są wyłącznie w Biurze Spółdzielni Mieszkaniowej w Janowcu wielkopolskim przy ulicy Gnieźnieńskiej 12/2.
    - Dane w postaci cyfrowej przetwarzane są w zabezpieczonych systemach informatycznych przechowywanych ww. siedzibie
    - Dane w postaci tradycyjnej przechowywane są w zamykanych na klucz szafach na terenie ww. siedziby.

10. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

Zestawienia zastosowanych środków technicznych i organizacyjnych przedstawiono w załączniku nr 9 do Polityki Bezpieczeństwa.

11. RETENCJA DANYCH

1. Dane których dotyczy procedura retencji
    a. Dane których usunięcia zażądał podmiot danych osobowych, a których dalsze przetwarzanie nie jest wymagane .
    b. Dane osobowe dla których cel przetwarzania upłynął.
2. Sposób przeprowadzenia retencji
    a. W systemach informatycznych – poprzez zamazanie losowymi znakami danych osobowych.
    b. W systemach tradycyjnych – poprzez zniszczenie dokumentacji papierowej zawierającej dane osobowe w niszczarce.
3. Okresy retencji dla danych których cel przetwarzania upłynął zawiera załącznik nr 6 do Polityki Bezpieczeństwa w polu Okres retencji. Okres wyrażony jest w latach po zakończeniu przetwarzania.

12. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

§ 1

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, określa:

- procedury przydziału haseł dla użytkowników, częstotliwość ich zmiany,
- procedury rozpoczynania i kończenia pracy,
- metodę i częstotliwość tworzenia kopii awaryjnych,
- metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,
- sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
- przenoszenie danych osobowych na nośnikach informacji,
- sposób postępowania w zakresie komunikacji w sieci komputerowej.

§ 2

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem" może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez Administratora systemu informatycznego na wniosek Administratora Danych Osobowych.
2. Identyfikator użytkownika składa się z unikalnej kombinacji liter, niezbędnej do jednoznacznej identyfikacji użytkownika.
3. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
4. Zmiana hasła następuje nie rzadziej niż co 30 dni.
5. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

§ 3

1. Każdorazowo przed rozpoczęciem pracy w systemie należy zalogować się korzystając z indywidualnego identyfikatora oraz hasła.
2. Kończąc pracę z systemem należy każdorazowo wylogować się i zamknąć system operacyjny.

§ 4

1. Kopie awaryjne tworzy się nie rzadziej niż raz na kwartał.
2. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.
3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

§ 5

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania.

§ 6

1. Przeglądu i konserwacji bieżącej dokonuje Administrator systemów informatycznych.
2. Przeglądu i sprawdzenia poprawności zbiorów danych osobowych zawierających dane osobowe dokonuje użytkownik.

§ 7

1. Zabrania się przenoszenia informacji na nośnikach informatyczne zawierających dane osobowe.

§ 8

1. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 10 minut nieaktywności użytkownika automatycznie wyłączają funkcje eksploatacji ekranu.

§ 9

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nieposiadających imiennego upoważnienia oraz nieuprawnionych do wglądu na podstawie indywidualnego zakresu czynności.
2. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 10

1. Zabrania się użytkownikom pracującym w systemie:

- udostępniania stacji roboczej osobom niezarejestrowanym w systemie,
- udostępniania indywidualnego hasła do systemu,
- udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia

z Administratorem systemu informatycznego,

- używania nielicencjonowanego oprogramowania.

§ 11

1. Każdy przypadek naruszenia ochrony danych osobowych zgłasza się Administratorowi Systemu Informatycznego, a w szczególności:

- naruszenia bezpieczeństwa systemu informatycznego,
- stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci), które mogą wskazywać na naruszenie bezpieczeństwa.
- użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
- usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
- usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
- przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody administratora danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
- udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służącym do przetwarzania danych osobowych,
- niezabezpieczeni hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
- przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
- przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

2. Obowiązek dokonania zgłoszenia, o którym mowa w ust. 1 spoczywa na każdym pracowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

13. ZAŁĄCZNIKI

Załącznik nr 1 – Ustanowienie Administratora Bezpieczeństwa Informacji

Załącznik nr 2 – Upoważnienie Administratora Bezpieczeństwa Informacji do nadawania upoważnień

Załącznik nr 3 – Ustanowienie Administratora Systemów Informatycznych

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy innej niż umowa o pracę

Załącznik nr 5 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

Załącznik nr 6 – Opis struktury zbiorów danych

Załącznik nr 7 – Ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 8 – Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych

Załącznik nr 9 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Załącznik nr 10 – Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających

Dokument sporządzono:	**Pełen podpis Administratora Danych:**	**Pieczęć**
Data: 30.06.2015 Aktualizacja 15.06.2018 Miejsce: Janowiec Wielkopolski		

ZAŁĄCZNIK NR 1 – USTANOWIENIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Niniejszym, zgodnie z art. 36a ust. 1 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i dyspozycją Rozdziału 2 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych – Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2,

wyznaczam

Panią/Pana ……..

na stanowisko **Administratora Bezpieczeństwa Informacji (ABI)** w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Bezpieczeństwa Informacji określone są Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 roku oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną dnia …/ … / …… (dd/mm/rrrr) w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2.

DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO ABI	DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

ZAŁĄCZNIK NR 2 – UPOWAŻNIENIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DO NADAWANIA UPOWAŻNIEŃ

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych – Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2,

upoważniam

Panią/Pana ……..

Administratora Bezpieczeństwa Informacji w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2 do nadawania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych.

DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO ABI	DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

ZAŁĄCZNIK NR 3 – USTANOWIENIE ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych – Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2,

wyznaczam

Panią/Pana ……..
na stanowisko **Administratora Systemów Informatycznych (ASI)** w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone są Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 roku oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną dnia …/ … / …… (dd/mm/rrrr) w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2.

DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO ASI	DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

ZAŁĄCZNIK NR 4A – WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH DLA OSÓB ZATRUDNIONYCH NA PODSTAWIE UMOWY O PRACĘ

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Bezpieczeństwa Informacji w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2, na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182**upoważniam:**

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r., poz. 1182), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2 wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania.

Data i podpis upoważniającego

Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2 (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

ZAŁĄCZNIK NR 4B – WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH DLA OSÓB ZATRUDNIONYCH NA PODSTAWIE INNEJ UMOWY NIŻ UMOWA O PRACĘ

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Bezpieczeństwa Informacji w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2, na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (T.j. Dz. U. z 2015 r. poz. 1309) **upoważniam:**

Imię i nazwisko upoważnionego	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 1309), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2 wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz odpowiedzialności cywilnej.

Upoważnienie jest ważne do odwołania.

....

Data i podpis upoważniającego Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Spółdzielni Mieszkaniowej w Janowcu Wielkopolskim przy ulicy Gnieźnieńskiej 12/2 (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych w związku z pełnioną przeze mnie funkcją i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu stosunku prawnego łączącego mnie z Administratorem Danych.

……..……..

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

ZAŁĄCZNIK NR 5 – WZÓR OŚWIADCZENIA O ZOBOWIĄZANIU SIĘ DO ZACHOWANIA POUFNOŚCI

…………………., dnia ……………..

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y . . . . zamieszkała/y w . . . . zatrudniona/y na stanowisku . . . . zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z …………………………….. Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

……………………………..……………………..
Podpis

ZAŁĄCZNIK NR 6 – OPIS STRUKTURY ZBIORÓW DANYCH

Nr	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi	Okres retencji
1.	Rejestr członków	---	Ewidencja członków spółdzielni mieszkaniowej oraz oczekujących	Osoby fizyczne	Imię, Nazwisko, Nr dokumentu, Nr Pesel, Adres Zamieszkania	Forma tradycyjna (papierowa)	50 lat
2.	Ewidencja lokatorów	Księgowość SM\WM ProVirtus	Naliczenia opłat czynszowych, rozliczenia opłat za media	Osoby fizyczne	Imię, Nazwisko, Adres Zamieszkania		5 lat
2.	Ewidencja kontrahentów	Księgowość SM\WM ProVirtus	Ewidencja faktur sprzedaży i zakupu	Jednoosobowa działalność gospodarcza	Imię, Nazwisko, Nr NIP, Nr Pesel, Adres działalności		5 lat
3.	Dokumentacja pracowników i współpracowników	---	Ewidencja zatrudnionych na umowy o prace i zlecenie. Rachuba Płac	Osoby fizyczne	Imię, Nazwisko, Nr dokumentu, Nr Pesel, Adres Zamieszkania	Forma tradycyjna (papierowa)	50 lat
4.	Dokumentacja pracowników i współpracowników	Program Płatnika	Ewidencja zatrudnionych na umowy o prace i zlecenie. Rachuba Ubezpieczeń ZUS	Osoby fizyczne	Imię, Nazwisko, Nr dokumentu, Nr Pesel, Adres Zamieszkania		50 lat
5.	Ewidencja kontrahentów	ADA	Naliczenia opłat czynszowych, rozliczenia opłat za media Do 31.12.2017 r.	Osoby fizyczne	Imię, Nazwisko, Nr dokumentu, Nr Pesel, Adres Zamieszkania		5 lat
6.	Ewidencja kredytobiorców	Kredyty	Rozliczenie kredytów mieszkaniowych	Osoby fizyczne	Imię, Nazwisko, Adres Zamieszkania		5 lat

ZAŁĄCZNIK NR 7 – EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator w systemie informatycznym	Nazwy zbiorów objętych zakresem upoważnienia
1.	Stanisław Birula	30.06.2015		----	Rejestr członków, Ewidencja lokatorów, Ewidencja kontrahentów, Dokumentacja pracowników i współpracowników, Ewidencja kredytobiorców
2.	Dorota Małęgowska	30.06.2015		Ksiegowa	Rejestr członków, Ewidencja lokatorów, Ewidencja kontrahentów, Dokumentacja pracowników i współpracowników, Ewidencja kredytobiorców
3.	Grzegorz Pinczyński	30.06.2015		----	Rejestr członków, Ewidencja lokatorów, Ewidencja kontrahentów
4.	Daniel Zaderecki	30.06.2015		Administrator	Ewidencja lokatorów, Ewidencja kontrahentów, Ewidencja kredytobiorców
5.					
6.					

ZAŁĄCZNIK NR 8 – WYKAZ PODMIOTÓW, KTÓRYM ADMINISTRATOR DANYCH POWIERZYŁ PRZETWARZANIE DANYCH OSOBOWYCH

	Adres / lokalizacja	Uwagi
Podmioty, którym Administrator Danych powierzył przetwarzanie danych osobowych	**---**	---
	---	---

ZAŁĄCZNIK NR 9 – OPIS ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

ŚRODKI TECHNICZNE

Środek ochrony technicznej i fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi** (niewzmacnianymi, nie przeciwpożarowymi).	TAK	
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za **pomocą krat, rolet lub folii antywłamaniowej.**	TAK	
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w **system alarmowy przeciwwłamaniowy.**	NIE	
4. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są **systemem kontroli dostępu.**	NIE	
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**	NIE	
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych** tam pracowników **nadzorowany przez służbę ochrony.**	NIE	
7. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej **niemetalowej szafie.**	NIE	
8. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie.**	TAK	
9. Zbiór danych osobowych w formie papierowej przechowywany jest **w zamkniętym sejfie lub kasie pancernej.**	NIE	
10. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**	NIE	

11. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w zamkniętej metalowej szafie**.	TAK	
17. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą **systemu przeciwpożarowego** i/lub **wolnostojącej gaśnicy.**	TAK	Gaśnica
18. Dokumenty zawierające dane osobowe **po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.**	TAK	

ŚRODKI ORGANIZACYJNE

Środek organizacyjny	Zastosowano (TAK / NIE)	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych	**TAK**	
Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych	**TAK**	
Wyznaczono Administratora Bezpieczeństwa Informacji	**TAK**	
Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych	**TAK**	
Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych	**TAK**	
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych	**TAK**	
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	**TAK**	
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy	**TAK**	
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym	**TAK**	
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	**TAK**	

ZAŁĄCZNIK NR 10 - PROTOKÓŁ Z KONTROLI PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH/ CZYNNOŚCI SPRAWDZAJĄCYCH

……..

miejscowość, data

PROTOKÓŁ

Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*

w zakresie ochrony danych osobowych

1. Nazwa kontrolowanej jednostki organizacyjnej:…….....
2. Zbiory danych osobowych, których przetwarzanie podlega kontroli: …….....
3. Data wykonania czynności kontrolnych:…….....
4. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne: …….....
5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej:……..……..……
   ….....…..……..
6. Ustalenia dokonane w trakcie czynności kontrolnych:……
   ……
   ……
   ……
   ……
   ……
   ……
   ……
7. Wnioski i zalecenia pokontrolne:
   ……
   ……
   ……
   ……
   ……
   ……

…….. ……...

(data i podpis osoby wykonującej czynności kontrolne) (data i podpis kierownika kontrolowanej kom. organizacyjnej)

Otrzymują:
1 x Kierownik kontrolowanej jednostki organizacyjnej
1 x Administrator Bezpieczeństwa Informacji

* niepotrzebne skreślić