POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

WERSJA III UAKTUALNIONA z dnia 17.03.2021r.

Zatwierdzona uchwałą Zarządu nr 13/2021

1.CEL POLITYKI

Polityka bezpieczeństwa danych osobowych wskazuje sposób działania oraz ustanawia zasady i reguły postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.
Niniejszy dokument określa zasady, które powinny być przestrzegane i stosowane w Spółdzielni Mieszkaniowej „Nasz Dom" w Bytomiu przez pracowników i współpracowników, którzy przetwarzają dane osobowe. Zgodnie ustawą z dnia 10 maja 2018r. o ochronie danych osobowych zwanej dalej ustawą, polityka bezpieczeństwa, odnosi się całościowo do problemu zabezpieczenia danych osobowych w tut. Spółdzielni Mieszkaniowej tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

2. ŹRÓDŁA WYMAGAŃ

1.1 Polityka bezpieczeństwa danych osobowych w Spółdzielni Mieszkaniowej „Nasz Dom" w Bytomiu, zwana dalej Polityką została wydana w zgodnie z:

- Ustawą z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. 2019 r. poz. 1781);
- Rozporządzeniem parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

1.2. Spółdzielnia Mieszkaniowa „Nasz Dom" prowadzi działalność, w szczególności na podstawie:

- Ustawy z dnia 16 września 1982 r. Prawo spółdzielcze (tekst ujednolicony Dz.U. 2018r., poz.1285 z późn.zm.),
- Ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (tekst jednolity Dz.U. z 2018r. , poz. 845 z późn.zm.),
- zarejestrowanego Statutu
- wydanych na podstawie Statutu regulaminów oraz instrukcji.
- W ramach regulacji monitoringu na podstawie:
  - Instrukcji monitoringu wizyjnego siedziby Spółdzielni Mieszkaniowej „Nasz Dom" w Bytomiu,
  - Regulamin monitoringu wizyjnego w dźwigach osobowych eksploatowanych w Spółdzielni Mieszkaniowej „Nasz Dom" w Bytomiu,
  - Regulamin monitoringu wizyjnego w budynkach Spółdzielni Mieszkaniowej „Nasz Dom" w Bytomiu przy ul. Hlonda 99,101,103.

3. DOKUMENTY POWIĄZANE

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Spółdzielni Mieszkaniowej „Nasz Dom" stanowi dokument związany z niniejszą Polityką i ma na celu zapewnienie właściwego przetwarzania danych osobowych.

4. ZAKRES STOSOWANIA

Politykę stosuje się do danych osobowych przetwarzanych w:

- formie papierowej (kartoteki, rejestry, segregatory),
- w systemach informatycznych wspomagających zarządzanie Spółdzielnią i powiązanych z nimi funkcjonalnie modułach, aplikacjach biurowych, również na zewnętrznych nośnikach informacji.

5. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

Przez bezpieczeństwo przetwarzania danych osobowych rozumie się zapewnienie:

- poufności — właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
- integralności — właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalności — właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Celem zapewnienia bezpieczeństwa danych osobowych wszyscy pracownicy i współpracownicy, zobowiązani są do przestrzegania i stosowania zasad wynikających z niniejszej Polityki Bezpieczeństwa Danych Osobowych.

6. DEFINICJE

6.1. **Administrator danych osobowych** – Spółdzielnia Mieszkaniowa „Nasz Dom" w Bytomiu, podmiot który decyduje o środkach i celach przetwarzania danych osobowych, zwany dalej SM „Nasz Dom".

Administrator danych osobowych odpowiada za zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a) zapewnienie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

b) nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych,

c) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

d) nadzór nad prowadzeniem rejestru zbiorów danych.

6.2. **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.

6.3. **Osoba upoważniona** – osoba posiadająca formalne upoważnienie wydane przez Administratora danych lub przez osobę przez niego wyznaczoną, uprawniona do przetwarzania danych osobowych.

6.4. **Przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, niezależnie od formy (papierowej lub elektronicznej).

6.5. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 10 maja 2018r. (Dz. U. 2019 r. poz. 1785 z późn.zm.)

6.6. **Zbiór danych osobowych** – dane osobowe zgromadzone w usystematyzowany sposób, pozwalający na łatwe dotarcie do konkretnej informacji, również w ramach zbiorów rozproszonych.

6.7. **Zbiór nieinformatyczny** - każdy posiadający strukturę zestaw danych o charakterze osobowym, prowadzony poza systemem informatycznym, w szczególności w formie kartotek, skorowidzów, ksiąg, wykazów lub innych zbiorów ewidencyjnych.

6.8. **Zbiór informatyczny** - każdy posiadający strukturę zestaw danych o charakterze osobowym, prowadzony w ramach systemów informatycznych.

7. ODPOWIEDZIALNOŚĆ

7.1. Kierownictwo.

Do obowiązków Kierownictwa należy zapewnienie świadomości wśród pracowników bezpieczeństwa przetwarzania danych osobowych, jego problematyki oraz wymagań.

Do obowiązków kierownictwa należy w szczególności:

- podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych;
- podział zadań i obowiązków związanych z organizacją ochrony danych osobowych,
- wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych;

- zapewnienie środków bezpieczeństwa przetwarzania danych osobowych;
- wskazanie podstaw prawnych do przetwarzania danych osobowych, od chwili zebrania danych osobowych, do chwili ich usunięcia;
- zapewnienie niezbędnych środków potrzebnych dla zachowania bezpieczeństwa przetwarzania danych osobowych.

7.2. Osoby upoważnione do przetwarzania danych.

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swoich stacji roboczych.

Do obowiązków osób upoważnionych należy w szczególności:

- przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa;
- postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;
- zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia;
- ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
- informowanie przełożonego o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe, który ma obowiązek poinformować osoby odpowiedzialne za nadzór nad przestrzeganiem zasad bezpieczeństwa.

8. ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

8.1. Podstawowe zasady.

8.1.1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane, w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych.

8.1.2. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

8.1.3. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

8.1.4. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

8.2. Procedury postępowania z danymi osobowymi.

8.2.1 Dostęp do danych osobowych przyznawany jest zgodnie z zasadą wiedzy koniecznej.

8.2.2 Dane osobowe należy chronić przed nieuprawnionym dostępem i modyfikacją.

8.2.3 Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

8.3. Upoważnienie do przetwarzania danych osobowych.

8.3.1 Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy Ustawy.

8.3.2 Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych.

8.3.3 Pracownik/ osoba z którą zawierana jest umowa cywilnoprawna/ stażysta/ praktykant w celu upoważnienia do przetwarzania danych osobowych winien złożyć w kadrach podpisane oświadczenie, którego wzór stanowi załącznik nr 1 do niniejszej Polityki.

8.3.4. Przełożony osoby, o której mowa w pkt 8.3.3 składa do kadr wniosek o nadanie lub cofnięcie uprawnień do przetwarzania danych osobowych, którego wzór stanowi załącznik nr 2 do niniejszej Polityki.

8.3.5. Na podstawie otrzymanego oświadczenia i wniosku Administrator Danych Osobowych upoważnia daną osobę do przetwarzania danych osobowych i wydaje upoważnienie, sporządzane wg wzoru stanowiącego załącznik nr 3 do niniejszej Polityki (część A – pracownicy, część B – członkowie organów samorządowych, część C - legenda).

W zakresie czynności osoby upoważnionej do przetwarzania danych osobowych określa się zakres dostępu do danych oraz odpowiedzialność za naruszenie ochrony tych danych.

8.3.6. Upoważnienia, o których mowa powyżej przechowywane są w aktach osobowych pracownika, w dokumentacji związanej z zawartą umową cywilnoprawną lub w innej dokumentacji, dotyczącej w szczególności stażystów i praktykantów. Upoważnienia obowiązują do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych.

8.4. Ewidencja osób upoważnionych.

8.4.1. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez osobę wyznaczoną przez Administratora Danych Osobowych i zawiera w szczególności:

- imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych;
- zakres upoważnienia do dostępu do systemów informatycznych,
- identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych;
- zakres upoważnienia do przetwarzania danych osobowych, nazwę zbiorów danych;
- datę nadania i odebrania uprawnień.

8.4.2. Przełożeni osób upoważnionych odpowiadają za natychmiastowe zgłoszenie do wyznaczonej przez Administratora Danych Osobowych osoby odpowiedzialnej za nadzór nad przestrzeganiem zasad bezpieczeństwa, osób które utraciły uprawnienia dostępu do danych osobowych.

8.4.3. Ewidencja osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 4 do niniejszej Polityki.

8.5. Zachowanie danych osobowych w tajemnicy.

Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia. Ponadto zobowiązane są do zmiany haseł zgodnie z obowiązującymi uregulowaniami wewnętrznymi.

8.6. Znajomość regulacji wewnętrznych.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są zapoznać się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w SM „Nasz Dom", w szczególności z Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym.

8.7. Zgodność .

8.7.1. Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w SM Nasz Dom, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

8.7.2. Zmiany niniejszej Polityki wymagają przeglądu innych powiązanych dokumentów dotyczących ochrony danych osobowych obowiązujących w SM Nasz Dom.

9. ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI

9.1. Bezpieczeństwo usług zewnętrznych.

Należy zapewnić aby usługi zewnętrzne były prowadzone zgodnie z wymaganiami prawa, wymaganiami umowy oraz zgodnie z zasadami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w Spółdzielni.

9.2. Powierzanie przetwarzania danych osobowych.

9.2.1. Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy.

9.2.2. W umowach stanowiących podstawę powierzenia przetwarzania danych albo eksploatacji systemu informatycznego lub części infrastruktury należy umieścić zobowiązanie podmiotu zewnętrznego zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych. Wzór zobowiązania opracowywany jest przez radcę prawnego i zatwierdzany przez Zarząd Spółdzielni.

9.2.3. Lista podmiotów, którym SM „Nasz Dom" powierza dane osobowe do przetwarzania stanowi załącznik nr 5 do niniejszej Polityki.

9.3. Udostępnianie danych osobowych.

9.3.1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.

9.3.2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora Danych Osobowych.

9.3.3. Wszelkie informacje dotyczące udostępnienia danych osobowych innym podmiotom (data, cel, zakres) należy przechowywać w postaci papierowej w formie oryginalnych pism, wniosków od uprawnionych podmiotów.

9.3.4. W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, wyznaczona przez Administratora Danych Osobowych osoba przygotowuje odpowiedź w ciągu 30 dni.

9.3.5. Udostępnienie danych osobowych przetwarzanych przez Spółdzielnię osobom fizycznym lub instytucjom publicznym może nastąpić jedynie na pisemnie umotywowany wniosek, chyba że przepis szczególny stanowi inaczej, z zaznaczeniem podstawy prawnej żądania udostępnienia danych.

9.3.6. Zarząd spółdzielni udostępnia dane osobowe członka Spółdzielni Walnemu Zgromadzeniu, Radzie Nadzorczej, Radzie Osiedla w przypadku, gdy w sprawie danego członka Spółdzielni toczy się postępowanie wewnątrzspółdzielcze w trybie określonym postanowieniami statutu spółdzielni. Dane osób nie będących członkami mogą zostać udostępnione tylko w takim zakresie, w jakim jest to konieczne dla realizacji zadań przyznanych tym organom.

9.3.7. Udostępnianie danych osobowych przetwarzanych przez SM „Nasz Dom" członkom Spółdzielni odbywa się w oparciu o przepisy ustawy o spółdzielniach mieszkaniowych i przepisy Statutu Spółdzielni.

9.3.8. Udostępnianie danych osobowych członkom Spółdzielni następuje na pisemny wniosek, którego wzór stanowi załącznik nr 6 do niniejszej Polityki. Wniosek powinien precyzyjnie określać o udostepnienie jakich danych wnosi wnioskodawca. Wzór wniosku znajduje się na stronie internetowej SM „Nasz Dom".

9.3.9. Dział DC prowadzi rejestr udostępnionych dokumentów. Rejestr ten powinien zawierać w szczególności datę przekazania lub udostępnienia dokumentów, wykaz udostępnionych dokumentów, informację czy członek otrzymał dokumenty w formie papierowej, czy przeglądał dokumenty, potwierdzenie przez członka (podpis) faktu udostępnienia dokumentów, imię, nazwisko i podpis pracownika, który nadzorował udostępnianie dokumentów.

9.3.10. Przeglądanie dokumentów powinno być nadzorowane przez pracownika działu, którego sprawa dotyczy.

9.3.11. Członek Spółdzielni ma prawo otrzymania odpisu Statutu i regulaminów oraz kopii uchwał organów Spółdzielni, protokołów obrad organów, protokołów lustracji, rocznych sprawozdań finansowych oraz faktur i umów zawieranych przez Spółdzielnię z osobami trzecimi.

9.3.12. Spółdzielnia może odmówić członkowi wglądu do umów zawieranych z osobami trzecimi o ile naruszałoby to prawa tych osób lub jeżeli istnieje uzasadniona obawa,

że członek wykorzysta pozyskane informacje w celach sprzecznych z interesem Spółdzielni i przez to wyrządzi Spółdzielni znaczną szkodę. Odmowa powinna być wyrażona na piśmie.

9.3.13. Członek Spółdzielni, któremu odmówiono wglądu do umów zawieranych przez Spółdzielnię z osobami trzecimi lub nie udostępniono wnioskowanych informacji, może złożyć wniosek do sądu rejestrowego o zobowiązanie Spółdzielni do udostępnienia tych dokumentów. Wniosek należy złożyć w terminie 7 dni od dnia doręczenia członkowi pisemnej odmowy.

9.3.14. Koszty sporządzania odpisów i kopii udostępnianych dokumentów, z wyjątkiem Statutu i regulaminów uchwalonych na podstawie Statutu, pokrywa członek Spółdzielni wnioskujący o ich otrzymanie. Koszty odpisów Statutu i regulaminów uchwalonych na jego podstawie są finansowane z funduszu danej nieruchomości budynkowej.

9.3.15. Opłatę za kopie dokumentów ustala Zarząd w formie uchwały.

10. ZAPEWNIENIA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

10.1. Obszar przetwarzania.

10.1.1. Dane osobowe mogą być przetwarzane w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Spółdzielnia prowadzi działalność oraz przy wykorzystaniu urządzeń mobilnych. Do pomieszczeń, zalicza się w szczególności:

- pomieszczenia biurowe w siedzibie Spółdzielni, w której zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych;
- pomieszczenia administracji, w których zlokalizowane są stacje robocze;
- pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe;
- pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.

10.1.2. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.

10.1.3. Osoby upoważnione zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich nieobecności w pomieszczeniu, a klucze nie mogą być pozostawione w zamku drzwi.

10.1.4. Wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych pomieszczeniach, które znajdują się w obszarach przetwarzania danych osobowych.

10.1.5. Niepotrzebne wydruki, dokumenty oraz płyty CD/DVD należy skutecznie niszczyć.

10.1.6. Przebywanie wewnątrz obszarów przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.

10.1.7. Szczegółowy wykaz obszarów przetwarzania danych osobowych znajduje się w załączniku nr 7 do niniejszej Polityki.

10.2. Fizyczna kontrola dostępu.

10.2.1. Klucze dostępowe, hasła itd., służące do uzyskania dostępu do systemów informatycznych służących do przetwarzania danych osobowych, należy zabezpieczać przed dostępem osób nieupoważnionych.

10.2.2. Dostęp interesantów do pomieszczeń, w których znajdują się systemy informatyczne służące do przetwarzania danych osobowych należy nadzorować przez cały czas ich pobytu.

10.2.3. Kończąc pracę, należy zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację, wydruki i elektroniczne nośniki informacji.

10.2.4. Monitory należy ustawić w taki sposób, aby uniemożliwiać podgląd wyświetlanych danych osobowych przez osoby nieuprawnione.

10.2.5. Korzystając z usług zewnętrznych podmiotów oferujących zbieranie i niszczenie papierów, urządzeń lub nośników zwierających dane osobowe, należy wybrać wykonawcę z odpowiednimi zabezpieczeniami i doświadczeniem.

10.3. Zabezpieczenie sprzętu komputerowego.

10.3.1. Przedsięwzięcia w zakresie zabezpieczenia sprzętu komputerowego:

1) dla zapewnienia ciągłości działania systemów informatycznych służących do przetwarzania danych osobowych stosuje się w nich zasilacze UPS, oprogramowanie wyprodukowane przez renomowanych producentów oraz zabezpiecza się sprzęt przed awarią zasilania lub zakłóceniami w sieci zasilającej;
2) zbiory danych osobowych oraz programy służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą albo celowym zniszczeniem poprzez wykonywanie kopii zapasowych;

10.3.2. Przedsięwzięcia w zakresie ochrony transmisji danych:

1) w celu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z Internetu stosuje się zabezpieczenia chroniące przed nieuprawnionym dostępem – hasła.
2) oprogramowanie antywirusowe.

10.3.3. Przedsięwzięcia w zakresie środków ochrony w ramach oprogramowania systemów:

1) w celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu informatycznego, w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło;
2) w przypadku, gdy do uwierzytelnienia użytkowników używa się identyfikatora i hasła, składa się ono z co najmniej 8 znaków, w szczególności zawiera małe i duże litery, cyfry oraz znaki specjalne;

3) hasła służące do uwierzytelniania w systemach informatycznych służących do przetwarzania danych osobowych są zmieniane co najmniej nie rzadziej niż co 30 dni;

10.3.4. Przedsięwzięcia w zakresie środków ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

1) w celu ochrony zbiorów danych osobowych prowadzonych w systemach informatycznych przed nieuprawnionym dostępem stosuje się mechanizmy kontroli dostępu do tych danych;
2) system powinien umożliwiać odnotowywanie w systemie informacji o identyfikatorze użytkownika, który wprowadził dane osobowe oraz dacie pierwszego wprowadzenia danych do systemu;

10.3.5. Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:

1) w celu ochrony danych osobowych przetwarzanych na stacjach roboczych na czas krótkotrwałego opuszczenia stanowiska pracy przez użytkownika systemu, należy stosować mechanizm blokady stacji roboczej zabezpieczony hasłem;
2) stosuje się mechanizmy kontroli dostępu użytkowników do systemów – nazwa użytkownika, hasło;
3) stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.
4) niedopuszczalne jest otwieranie plików niewiadomego pochodzenia np. pobieranych z poczty elektronicznej, stron internetowych lub serwerów FTP.
5) nie wykorzystuje się powierzonego sprzętu i oprogramowania do celów prywatnych.

10.4.Środki organizacyjne zapewniające bezpieczeństwo.

Przedsięwzięcia w zakresie środków organizacyjnych służące bezpieczeństwu przetwarzania danych:

1) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
2) dostęp do danych osobowych możliwy jest po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych wydanego przez upoważnione osoby;
3) wprowadzono Instrukcję zarządzania systemem informatycznym,
4) monitoruje się wdrożone zabezpieczenia systemu informatycznego.

11. OCENA RYZYKA I PRZEGLĄDY

11.1. Ocena ryzyka.

Systemy informatyczne i aplikacje powinny być poddawane ocenie ryzyka pod kątem identyfikacji zagrożeń dla bezpieczeństwa przetwarzania danych osobowych co najmniej raz na trzy lata. Ocena ryzyka powinna być również przeprowadzana przy dużych zmianach procesów zarządzania, systemów informatycznych i aplikacji.

11.2. Przeglądy bezpieczeństwa.

11.2.1. Przeglądy bezpieczeństwa przetwarzania danych osobowych powinny być przeprowadzane okresowo, co najmniej raz na rok w celu określenia wymaganego poziomu zabezpieczeń pozwalającego na ograniczenie ryzyka do poziomu akceptowalnego.

11.2.2. Przeglądy zgodności z zasadami bezpieczeństwa przetwarzania danych osobowych urządzeń informatycznych oraz sieci teleinformatycznych należy przeprowadzać okresowo, zgodnie z potrzebami.

11.2.3. Minimum raz na rok należy dokonywać przeglądu oprogramowania zainstalowanego na stanowiskach komputerowych.

11.2.4. O terminie audytu i przeglądu oprogramowania oraz jego zakresie decyduje Zarząd.

11.2.5. Zarząd dokonuje wyboru komisji lub osób przeprowadzających audyt lub przegląd oprogramowania.

11.2.6. Z przeprowadzonego audytu lub przeglądu sporządza się raport, który przedkładany jest Zarządowi.

11.2.7. Po przeprowadzeniu rocznego audytu i przeglądu określa się i szacuje ryzyka naruszenia bezpieczeństwa danych osobowych.

12. ZARZĄDZANIE INCYDENTAMI

12.1. Monitorowanie incydentów.

12.1.1. Incydenty związane z bezpieczeństwem przetwarzania danych osobowych powinny być wykrywane, rejestrowane i monitorowane w celu ich zidentyfikowania i zapobiegania ich wystąpieniu w przyszłości.

12.1.2. Zdarzenia systemowe powinny być przechowywane jako materiał dowodowy zaistniałych incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.

12.1.3. Użytkownicy systemów powinni znać i przestrzegać zasady zgłaszania incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.

12.2. Zgłaszanie incydentów .

Zaistniałe zdarzenia związane z naruszeniem lub podejrzeniem naruszenia bezpieczeństwa przetwarzania danych osobowych takie jak np. utrata integralności, niedostępność, awarie, uszkodzenia, ostrzeżenia i alarmy bezpieczeństwa systemów informatycznych, urządzeń teleinformatycznych oraz danych powinny być niezwłocznie zgłaszane osobie wyznaczonej przez Administratora danych Osobowych.

Ze zgłoszenia wyznaczona przez Administratora Danych Osobowych osoba sporządza raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych, którego wzór zamieszczony jest w załączniku nr 8 do niniejszej Polityki.

Raporty wpisywane są do rejestru naruszeń bezpieczeństwa zasad ochrony danych osobowych.

13. ZBIORY DANYCH OSOBOWYCH

13.1. Wykaz zbiorów danych osobowych.

13.1.1. Dokumentacja zbiorów danych osobowych jest prowadzona przez Administratora Danych osobowych i stanowi załącznik nr 9 do niniejszej Polityki.

13.1.2. Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w postaci papierowej, które są zlokalizowane w pomieszczeniach lub części pomieszczeń należących do obszaru przetwarzania danych osobowych.

14. POSTANOWIENIA KOŃCOWE

14.1.1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia umowy osobie, która dopuściła się naruszenia.

14.1.2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. 2019r. poz. 1781) oraz przepisy wykonawcze do tej Ustawy.

14.1.3. Pracownicy SM „Nasz Dom" w Bytomiu zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Spółdzielni użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

Polityka bezpieczeństwa danych osobowych – wersja III uaktualniona została zatwierdzona uchwałą Zarządu nr 13/2021 w dniu 17.03.2021r.

Traci moc Polityka bezpieczeństwa danych osobowych zatwierdzona uchwałą Zarządu nr 92/2019 w dniu 29 października 2019r. z późniejszymi zmianami.

ZASTĘPCA PREZESA ZARZĄDU
ds. EKSPLOATACJI
mgr inż. Piotr Podgórski

PREZES ZARZĄDU
GŁÓWNY KSIĘGOWY
mgr Jolanta Wójcik-Browko

.....

Zarząd Spółdzielni Mieszkaniowej
„Nasz Dom" w Bytomiu

Oprac.
Magdalena Ferfecka