Załącznik nr 1
do Uchwały Zarządu
nr 69 z dnia 15.09.2016r.

POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ W LUBANIU

Pieczęć firmowa:	Podpis Administratora Danych Osobowych (Zarząd Spółdzielni)	Data:
SPÓŁDZIELNIA MIESZKANIOWA ul. B. Chrobrego 3, 59-800 Lubań tel./fax 75-722-23-56 NIP 613-000-40-05		15-09-2016

Podpis Inspektora Bezpieczeństwa Informacji	Data:	Podpis Administratora Systemu Informatycznego	Data:
Bernat	15-09-2016		15-09-2016

Spis treści

Spis treści 2
Wstęp 3
Definicje 3
Inspektor Bezpieczeństwa Informacji 4
Ewidencja obszarów przetwarzania, zbiorów danych oraz oprogramowania 5
1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe. 5
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. 5
3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. 5
4. Sposób przepływu danych pomiędzy poszczególnymi systemami. 6
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych 6
Procedura dostępu podmiotów zewnętrznych 7
Instrukcja alarmowa 7
Szkolenia użytkowników 8
Postanowienia końcowe 9

Wstęp

Realizując postanowienia Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jedn. Dz. U. 2014r., poz. 1182 z późn. zm.) oraz wydane w oparciu o delegacje ustawową przepisy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. (Dz. U. 2004r. Nr. 100 poz. 1024 z późn. zm.) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Oprócz niniejszej „Polityki" opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją zarządzania systemem informatycznym przetwarzającym dane osobowe". Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez samych użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. Polityka – rozumie się przez to niniejszą „Politykę bezpieczeństwa ochrony danych osobowych".
2. Administrator Danych Osobowych – Spółdzielnia Mieszkaniowa w Lubaniu, ul. B.Chrobrego 3, decydujący o celach i środkach przetwarzania danych osobowych;
3. Inspektor Bezpieczeństwa Informacji (IBI) – wyznaczony przez Administratora Danych Osobowych, odpowiedzialny za organizację ochrony danych osobowych. (Załącznik nr 1)
4. Ustawa – rozumie się przez to Ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jedn. Dz. U. 2014r., poz. 1182 z późn. zm.)

5. Rozporządzenie – rozumie się przez to Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 1998r. Nr 80, poz. 521 z późn. zm.)
6. Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
7. Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów.
8. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
9. Zgoda osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
10. Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych danych. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe.
11. Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie.
12. System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
13. Inspektor systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.
14. Użytkownik – pracownik posiadający uprawnienia do pracy w systemie informatycznym zgodnie ze swoim zakresem obowiązków.
15. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
16. Nośnik komputerowy (wymienny) – nośnik służący do zapisu i przechowywania informacji np. CD, dyskietki, dyski twarde.

Inspektor Bezpieczeństwa Informacji

Do najważniejszych obowiązków Inspektora Bezpieczeństwa Informacji należy:

1. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
   b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 „Ustawy”, oraz przestrzegania zasad w niej określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
2. prowadzenie „Rejestru zbiorów danych osobowych” przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 „Ustawy”, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 (Załącznik nr 2).

3. zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej „Polityki”,
4. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych dla osób przetwarzających te dane wg wzoru, stanowiącego Załącznik nr 3a, 3b i 3c,
5. prowadzenie ,,Ewidencji osób upoważnionych do przetwarzania danych osobowych” (Załącznik nr 4),
6. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
9. zgłaszanie Administratorowi danych osobowych wszelkich uwag i spostrzeżeń dotyczących przestrzegania przepisów o ochronie danych osobowych, w szczególności sytuacji zagrożeń skutecznej ochrony tych danych.

Inspektor Bezpieczeństwa Informacji ma prawo :

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji,
2. wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
3. żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4. żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5. żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

Ewidencja obszarów przetwarzania, zbiorów danych oraz oprogramowania

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe.

Obszarem przetwarzania danych osobowych są biura Spółdzielni Mieszkaniowej, położone na I piętrze oraz w piwnicy (archiwa) budynku przy ul. B.Chrobrego 3, 59-800 Lubań oraz biura Grupy Remontowo-Budowlanej (GRB) ul. Łączna 7, 59-800 Lubań (dotyczy tylko zbiorów danych pracowników Spółdzielni w wersji papierowej).

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisany jest w „Rejestrze zbiorów danych osobowych w SM Lubań”.

3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Opis struktury zbiorów danych osobowych przedstawiono w „Instrukcji obsługi” zintegrowanego systemu informatycznego używanego w Spółdzielni Mieszkaniowej w Lubaniu, jakim jest program Comarch-OPTIMA wraz z nakładką „Aquila”.

4. Sposób przepływu danych pomiędzy poszczególnymi systemami.

Dane osobowe przetwarzane są w Spółdzielni Mieszkaniowej w Lubaniu w zintegrowanym systemie Comarch-OPTIMA wraz z nakładką „Aquila" i przepływy danych występują jedynie wewnątrz tego systemu. Jeśli zachodzi taka potrzeba, dane eksportowane są do arkuszy kalkulacyjnych Excel.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

A) Zabezpieczenia organizacyjne:

1. został wyznaczony Inspektor Bezpieczeństwa Informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych;
2. została opracowana i wdrożona „Polityka bezpieczeństwa";
3. została opracowana i wdrożona „Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe";
4. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez Inspektora Danych;
5. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
6. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
7. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
8. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
9. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
10. stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.

B) Zabezpieczenia ochrony fizycznej danych osobowych:

1. dostęp do poszczególnych pomieszczeń obszaru przetwarzania danych, opisanego powyżej, jest chroniony trzema drzwiami (drzwi zewnętrzne budynku, drzwi zewnętrzne biura, drzwi pomieszczenia), z których dwa pierwsze zaopatrzone są w 2 zamki, a trzecie w pojedynczy zamek wielozapadkowy; wszystkie biura znajdują się na I piętrze budynku, natomiast archiwa znajdujące się w piwnicach mają dodatkowe zabezpieczenie w postaci metalowej kraty zamykanej na 2 kłódki z zamkiem wielozapadkowym; biura bazy GRB chronione są drzwiami zabezpieczonymi zamkami wielozapadkowymi;
2. obszar przetwarzania danych jest chroniony systemem alarmowym z indywidualnymi kodami dostępu dla osób upoważnionych, a baza GRB także systemem monitoringu wizyjnego z powiadomieniem grupy interwencyjnej,
3. pomieszczenie, w których znajdują się serwery, zabezpieczone są drzwiami antywłamaniowymi, pomieszczenie to jest pomieszczeniem wewnętrznym, położonym na I piętrze i nie posiada okien,

4. w pomieszczeniach biurowych klienci i inne osoby nie zatrudnione w Spółdzielni Mieszkaniowej mogą przebywać tylko w obecności pracownika Spółdzielni.

C) Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w „Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe".

D) Zabezpieczenia narzędzi programowych i baz danych:
Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w „Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe".

Procedura dostępu podmiotów zewnętrznych

Celem procedury jest zapewnienie bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, gdy cel i zakres tego przetwarzania określa Administrator Danych.

1. Inspektor Bezpieczeństwa Informacji prowadzi rejestr podmiotów zewnętrznych, którym Administrator udostępnia dane osobowe oraz podmiotów, którym powierzono przetwarzanie danych osobowych w formie usługi zewnętrznej. Wzór rejestru stanowi Załącznik nr 5 do niniejszej Instrukcji.
2. Administrator Danych udostępnia dane osobowe będące w jego obszarze fizycznym podmiotom zewnętrznym w oparciu o umowę, której wzór zawarto w Załączniku nr 6 do niniejszej Instrukcji.
3. Podmiot zewnętrzny zobowiązany jest do zachowania poufności udostępnionych danych i przetwarzania ich zgodnie z celem umowy.

Instrukcja alarmowa

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub Inspektora Bezpieczeństwa Informacji;
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),
   c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia zagrożenia, Inspektor Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
   a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   b. inicjuje ewentualne działania dyscyplinarne,
   c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
   d. dokumentuje prowadzone postępowania.
5. W przypadku stwierdzenia incydentu (naruszenia), Inspektor Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
   a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   b. zabezpiecza ewentualne dowody,
   c. ustala osoby odpowiedzialne za naruszenie,
   d. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   e. inicjuje działania dyscyplinarne,
   f. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   g. dokumentuje prowadzone postępowania.

Szkolenia użytkowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych zgodnie z nadawanym upoważnieniem.
2. Za przeprowadzenie szkolenia odpowiada IBI, a za jego zorganizowanie odpowiada przełożony szkolonych użytkowników.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u ADO, a także o zobowiązaniu się do ich przestrzegania. Szczegółowy zakres szkolenia znajduje się w Załączniku nr 7.

Postanowienia końcowe

1. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią Polityki bezpieczeństwa każdego użytkownika.
2. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
6. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jedn. Dz. U. 2014r., poz. 1182 z późn. zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
7. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tekst jedn. Dz. U. 2014r., poz. 1182 z późn. zm.) oraz wydane na jej podstawie akty wykonawcze.