POLITYKA BEZPIECZEŃSTWA

W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

w

PILSKIEJ SPÓŁDZIELNI MIESZKANIOWEJ LOKATORSKO-WŁASNOŚCIOWEJ w PILE

SPIS TREŚCI

§ 1

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r. poz. 1182) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. z 2004 r. Nr 100, poz. 1024. Opracowany dokument jest zgodny z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 2

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile, a w szczególności:

1. ochrona danych osobowych przetwarzanych i gromadzonych w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile i dotyczy:
   a) zabezpieczenia przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi,
   b) metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach,
   c) procedur niszczenia niepotrzebnych wydruków lub nośników z danymi,
   d) ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane,
   e) określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis zewnętrzny,
2. zmniejszenie ryzyka utraty informacji,
3. określenia zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych,
4. podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych danych.

§ 3

Niniejszy dokument opisuje reguły dotyczące zabezpieczenia danych osobowych przetwarzanych zarówno w systemach informatycznych jak i w formie tradycyjnej, w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Spółdzielni. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone uprawnienia oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

§ 4

Ze względu na wagę problemów związanych z ochroną prawa do prywatności, a w szczególności prawa osób fizycznych powierzających swoje dane osobowe, do właściwej i skutecznej ochrony tych danych należy:

1. podjąć wszelkie niezbędne działania dla ochrony praw i usprawiedliwionych interesów jednostki związane z bezpieczeństwem danych osobowych,
2. podnosić świadomość oraz kwalifikacje osób przetwarzających dane osobowe w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile w zakresie problematyki bezpieczeństwa tych danych,
3. traktować obowiązki przy przetwarzaniu danych osobowych, przez osoby zatrudnione w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile, jako należące do kategorii podstawowych obowiązków pracowniczych,

4. stałe doskonalić i rozwijać nowoczesne metody przetwarzania danych oraz podejmować i rozwijać organizacyjne, techniczne i informatyczne środki ochrony tych danych tak, aby skutecznie zapobiegać zagrożeniom związanym z:
   a) nieautoryzowanym dostępem, wykradaniem bądź niszczeniem danych przez wszelkiego rodzaju mechanizmy i programy szpiegujące, wirusy komputerowe, konie trojańskie i inne niepożądane oprogramowanie,
   b) dostępem do nieautoryzowanych i niezabezpieczonych stron internetowych, mogących posiadać skrypty pozwalające wykradać zasoby komputera, który się z nimi łączy,
   c) atakami z sieci uniemożliwiającymi przetwarzanie danych (ataki typu DoS na serwer/serwery) oraz spamem,
   d) użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania danych poza Spółdzielnię,
   e) możliwością niekontrolowanego kopiowania danych na zewnętrzne nośniki,
   f) działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,
   g) lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez zabezpieczenia,
   h) brakiem świadomości niebezpieczeństwa przy dopuszczaniu osób postronnych do swojego stanowiska pracy,
   i) kradzieżą sprzętu lub nośników z danymi,
   j) kradzieżami tożsamości umożliwiającymi podszywanie się pod inną osobę,
   k) przekazywaniem niezabezpieczonego sprzętu komputerowego do serwisu zewnętrznego,
   l) innymi zagrożeniami mogącymi wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.

ZAKRES STOSOWANIA POLITYKI BEZPIECZEŃSTWA

§ 5

Zasady określone przez niniejszy dokument mają zastosowanie do całego systemu przetwarzania danych w tym do systemu informatycznego, a w szczególności do:

1. wszystkich pracowników Spółdzielni, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie,
2. wszystkich istniejących obecnie lub wdrażanych w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,
3. informacji będących własnością Spółdzielni, o ile zostały przekazane do Spółdzielni na podstawie umów lub porozumień ,
4. wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,
5. wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

DEFINICJE

§ 6

Następujące pojęcia użyte w niniejszym dokumencie oznaczają:

dane osobowe - to każda informacja dotycząca osoby fizycznej, pozwalająca na identyfikacje tożsamości tej osoby,

przetwarzanie danych - to wszelkie operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

administrator danych – Administrator Danych Osobowych - *zarząd* Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile,

administrator bezpieczeństwa informacji - ABI - wyznaczona osoba odpowiedzialna za nadzorowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w dokumentacji PSM L-W w Pile,

administrator systemu informatycznego - ASI - informatyk odpowiedzialny za sprawne funkcjonowanie sieci komputerowej i oprogramowania zainstalowanego na serwerach i stacjach roboczych,

osoba upoważniona - użytkownik - osoba posiadająca upoważnienie wydane przez administratora danych i dopuszczona w zakresie w nim wskazanym jako użytkownik do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład,

użytkownik danych – każdy pracownik Spółdzielni, który wykonując czynności służbowe, przetwarza dane osobowe, tzn. wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, czy usuwanie,

osoba uprawniona – osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych do wykonywania w jego imieniu określonych czynności,

osoba trzecia - to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez administratora w zakresie czynności przekraczających ramy udzielonego jej upoważnienia,

sieć telekomunikacyjna – sieć o definicji zawartej w Ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2004r. Nr 171, poz. 1800, z późniejszymi zmianami),

sieć lokalna – połączenie funkcjonujących w Spółdzielni systemów informatycznych i stacji roboczych przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom dostęp do danych znajdujących się w tym systemie,

system informatyczny – zespół współpracujących ze sobą urządzeń, programów, połączeń sieciowych i narzędzi programowych zastosowanych w celu przetwarzania danych,

bezpieczeństwo systemu informatycznego – wdrożone przez ABI lub osobę przez niego uprawnioną, środki organizacyjne i techniczne w celu zabezpieczenia oraz ochrony danych przed nieautoryzowanym dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem,

system przetwarzania danych – ta część systemu informatycznego oraz te procedury przetwarzania dokumentów papierowych, które razem tworzą system współpracujących ze sobą mechanizmów wykorzystywanych przy przetwarzaniu danych w Spółdzielni,

integralność danych – właściwość zapewniającą, że dane osobowe nie zostały zmienione
lub zniszczone w sposób nieautoryzowany,

poufność danych – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom i osobom,

zbiór danych osobowych – każdy posiadający strukturę logiczną zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

ZAPISY OGÓLNE

§ 7

Zarząd Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile mając na celu zabezpieczenia danych gromadzonych i przetwarzanych w Spółdzielni oraz dla podniesienia bezpieczeństwa w przetwarzających je systemach informatycznych, a w szczególności w celu ochrony danych osobowych, wprowadza określone w niniejszym dokumencie zasady postępowania.

§ 8

Zarząd Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile 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:

1. przetwarzane zgodnie z prawem,
2. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
3. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 9

Polityka bezpieczeństwa w zakresie ochrony danych osobowych odnosi się do danych osobowych przetwarzanych w zbiorach danych:

1. tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
2. w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.

§ 10

Dane osobowe w Spółdzielni przetwarzane są w celu:

1. realizacji statutowych zadań i obowiązków,
2. zapewnienia prawidłowej, zgodnej z prawem polityki personalnej,
3. dla realizacji innych usprawiedliwionych celów i zadań Spółdzielni z zapewnieniem poszanowania praw i wolności osób powierzających Spółdzielni swoje dane.

§ 11

Wprowadzona zostaje następująca klasyfikacja informacji :

1. **Informacje niejawne** – informacje, których ujawnienie może spowodować istotne straty finansowe lub problemy prawne i co do których stosuje się przepisy o ochronie informacji niejawnych lub o ochronie danych osobowych np.:
   a) dane osobowe petentów i zatrudnionych pracowników,
   b) dane o wynagrodzeniach i historii zatrudnienia pracowników,
2. **Informacje wewnętrzne** – wszystkie informacje wytworzone wewnątrz Spółdzielni, których przetwarzanie i udostępnianie podlega restrykcjom z uwagi na szczególne znaczenie dla pracodawcy (właściciela informacji), nieprzeznaczone do przedstawienia na forum publicznym;
   a) informacje **wewnętrzne dostępne** – informacje dostępne dla wszystkich pracowników Spółdzielni,
   b) informacje **wewnętrzne zastrzeżone** – informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe,
   c) informacje **stanowiące tajemnicę pracodawcy** – informacje, których upublicznienie może narazić Spółdzielnię na szkodę,
3. **Informacje publiczne/jawne** – informacje, które mogą być przedstawione na forum i do wiadomości publicznej.

ZAPISY SZCZEGÓŁOWE

§ 12

Zarząd Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile jako administrator danych osobowych przetwarza przedmiotowe dane z poszanowaniem obowiązujących w tym zakresie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2014r. Dz. U. poz.1182) oraz przepisów wykonawczych z nią związanych oraz innych przepisów, ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.

§ 13

Szczególną ochroną Zarząd Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile obejmuje wrażliwe dane osobowe wymienione w art. 27 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Przetwarzanie danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sadowym lub administracyjnym dopuszczalne jest tylko w związku z realizacja celów statutowych Spółdzielni i w granicach wynikających z przepisów art. 27 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

POWOŁANIE I OBOWIĄZKI ADMINISTRATORÓW

§ 14

Zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r. , poz. 1182), za prawidłowe przetwarzanie danych osobowych w systemach służących do przetwarzania danych osobowych jest Administrator Danych Osobowych.

§ 15

Administratorem Danych Osobowych w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile jest Zarząd Spółdzielni.

§ 16

Do zadań Administratora Danych Osobowych należy:

1. prawna odpowiedzialność za funkcjonowanie Spółdzielni, a w szczególności za przestrzeganie wymagań związanych z bezpieczeństwem danych osobowych,
2. zatwierdzanie i publikowanie dokumentów związanych z ochroną informacji,
3. zapewnienie wsparcia organizacyjno-finansowego przy wdrażaniu i dalszym rozwijaniu mechanizmów zabezpieczenia informacji i systemu informatycznego,
4. odpowiednie zabezpieczenie pomieszczeń w których przetwarza się lub przechowuje dane osobowe,
5. poinformowanie pracowników o prawnych i pracowniczych konsekwencji działań będących naruszeniem bezpieczeństwa danych osobowych,
6. ciągłe poszerzanie wiedzy i świadomości pracowników na temat bezpieczeństwa danych osobowych,
7. aktywne reagowanie na incydenty w zakresie naruszenia bezpieczeństwa systemu informatycznego i wyciąganie konsekwencji dyscyplinarnych wobec pracowników których zaniedbania doprowadziły do naruszenia bezpieczeństwa danych,
8. zarząd Spółdzielni powołuje Administratora Bezpieczeństwa Informacji, osobę upoważnioną do zastępowania ABI oraz Administratora Systemu Informatycznego.

§ 17

Do zadań Administratora Bezpieczeństwa Informacji należy:

1. ochrona bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Spółdzielni,
2. ciągłe doskonalenie sposobu realizacji mechanizmów ochrony danych osobowych z uwzględnieniem specyfiki pracy poszczególnych komórek organizacyjnych,
3. podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
4. niezwłocznego informowania Administratora lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
5. nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

§ 18

Do zadań Administratora Systemu Informatycznego należy:

1. zapewnienie użytkownikom możliwości bezpiecznego korzystania ze środowiska informatycznego, w sposób zapewniający identyfikację każdego z użytkowników,
2. nadanie odpowiedniego poziomu uprawnień użytkownikom, adekwatnie do wykonywanych obowiązków służbowych, a określonych w upoważnieniu ADO,
3. wdrożenie odpowiednich zabezpieczeń w administrowanym środowisku informatycznym,
4. tworzenie kopii zapasowych danych systemu informatycznego,
5. instalacja i aktualizacja oprogramowania zgodnego z posiadanymi przez Spółdzielnię licencjami,
6. ciągłe monitorowanie bezpieczeństwa środowiska informatycznego, ze szczególnym uwzględnieniem aktualności systemów operacyjnych serwerów, oraz definicji wirusów programów antywirusowych,
7. monitorowanie działania środowiska informatycznego, a w przypadku wykrycia zagrożeń przekazywanie tych informacji ABI lub ADO,
8. reagowanie na incydenty w zakresie bezpieczeństwa , usuwania ich skutków i podejmowanie działań przeciwdziałających pojawieniu się tych incydentów w przyszłości,
9. kontrolowanie przestrzegania zasad bezpiecznego przetwarzania danych w systemie informatycznym,
10. szkolenie użytkowników w zakresie bezpiecznego przetwarzania danych osobowych,
11. regularne przeglądy infrastruktury informatycznej, m.in.:
    a. prawidłowego rozmieszczenia stacji roboczych służących do przetwarzania danych,
    b. kontrola legalności oprogramowania zainstalowanego na stacjach roboczych,
    c. aktualności systemów operacyjnych stacji roboczych oraz definicji programów antywirusowych,
    d. wykazu pomieszczeń dopuszczonych do przetwarzania danych,

ZASADY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH

§ 19

1. Dostęp pracowników do systemu informatycznego, programów przetwarzających dane osobowe oraz urządzeń z nimi powiązanych możliwy jest wyłącznie na podstawie upoważnienia wydanego przez ADO.
2. Wniosek o wydanie upoważnienia do przetwarzania danych, składany jest w formie pisemnej na wniosek przełożonego pracownika do ADO lub ABI.
3. Przed dopuszczeniem do pracy w systemie informatycznym, każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych oraz niniejszą polityką bezpieczeństwa. Fakt ten pracownik potwierdza własnoręcznym podpisem na stosownym wykazie.
4. Użytkownicy danych osobowych obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia.
5. Osoba przetwarzająca dane osobowe składa oświadczenie o zapoznaniu się z przepisami o odpowiedzialności karnej i dyscyplinarnej za naruszenie bezpieczeństwa danych osobowych oraz zachowaniu tajemnicy służbowej. Oświadczenie to przechowywane jest w aktach osobowych pracownika.

OBOWIĄZKI PRACOWNIKÓW W ZAKRESIE ZACHOWANIA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH

§ 19

1. Każdy pracownik Spółdzielni powinien:
    a) przestrzegać zasad zachowania bezpieczeństwa podczas pracy w systemie informatycznym,
    b) chronić przed niedozwolonymi zmianami, nieupoważnionym dostępem, rozpowszechnianiem, uszkodzeniem lub zniszczeniem wszelkich danych będących w posiadaniu Spółdzielni,
    c) niezwłocznie informować o incydentach w zakresie bezpieczeństwa systemu informatycznego,
    d) wykonywać polecenia ADO, ABI, ASI w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego.

2. Zabrania się:

a) informowania kogokolwiek o haśle logowania do systemu informatycznego,
b) zapisywania identyfikatorów i haseł dostępu do systemu informatycznego i programów w miejscach, które umożliwiłyby osobom trzecim zapoznanie się z nimi,
c) udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej jak i wydruków) osobom nieupoważnionym,
d) wykorzystywania komputerów i zasobów sieci teleinformatycznej w celach innych niż służbowe,
e) samodzielnego instalowania i używania programów komputerowych,
f) kopiowania programów komputerowych w całości lub w części,
g) rozpowszechniania programów komputerowych lub ich kopii, będących własnością Spółdzielni,
h) przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,
i) udostępniania osobom postronnym programów komputerowych i danych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu,
j) wykorzystywania oprogramowania lub materiałów ściąganych z Internetu do masowego rozpowszechniania bez wyraźnego upoważnienia ABI lub ASI,
k) uruchamiania programów otrzymanych pocztą elektroniczną oraz odczytywania listów o wątpliwej treści,
l) kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez zgody ABI.

3. W szczególności w celu zwiększenia bezpieczeństwa danych i sieci komputerowej:
   a) ogranicza się w siedzibie Spółdzielni obieg dyskietek, pendrive-ów i innych nośników informatycznych poprzez ich oznaczenie i zarejestrowanie w ewidencji wewnętrznej Spółdzielni,
   b) wprowadza się zakaz obiegu nośników nie oznakowanych w sposób, o którym mowa w ust.1, a wszystkie nośniki pochodzące od jednostek zewnętrznych mogą być wykorzystane tylko do jednorazowego odczytu ich zawartości po uprzednim sprawdzeniu programem antywirusowym.
4. Wprowadza się mechanizmy zmierzające do poprawy jakości pracy w systemie informatycznym Spółdzielni, polegające w szczególności na ograniczeniu możliwości pobierania określonych danych z Internetu, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnej treści oraz kontroli antywirusowej.

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

§ 20

1. Podział zagrożeń:
   a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu. Ciągłość systemu zostaje zakłócona, nie dochodzi jednak do naruszenia poufności danych,
   b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   c) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
      - ✓ nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
      - ✓ nieuprawniony dostąp do systemu z jego wnętrza,
      - ✓ nieuprawniony przekaz danych,
      - ✓ pogorszenie jakości sprzętu i oprogramowania,
      - ✓ bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
d) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
f) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
g) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
h) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
i) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
j) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
k) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
l) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
m) rażąco naruszono dyscypliną pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

PROCEDURY POSTĘPOWANIA W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO LUB JEGO SKŁADNIKÓW

§ 21

1. W przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń systemu informatycznego, należy natychmiast powiadomić o tym fakcie bezpośredniego przełożonego, ABI oraz ASI. O wystąpieniu naruszenia zabezpieczeń systemu mogą świadczyć:
   a) ślady włamania lub prób włamania do pomieszczeń w których znajdują się elementy środowiska komputerowego,
   b) stan stacji roboczej (problemy z uruchomieniem, rozkręcona obudowa),
   c) zniszczenie elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,
   d) nieprawidłowe funkcjonowanie systemu (np. komunikaty informujące o niespójności i błędach w danych, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach, niestandardowe komunikaty),
2. ABI lub inna upoważniona przez niego osoba powinna w pierwszej kolejności:
   a) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
   b) zabezpieczyć miejsce zdarzenia przed ingerencją osób trzecich, aż do jego pełnego wyjaśnienia lub udokumentować jego stan za pomocą np. zdjęć z telefonu komórkowego bądź aparatu czy notatki z opisem,
   c) niezwłocznie podjąć odpowiednie kroki w celu:
      I. powstrzymania lub ograniczenia dostępu do systemu i danych osoby niepowołanej,
      II. zminimalizowania okoliczności mogących sprzyjać dalszemu powstawaniu szkód,
      III. zabezpieczenia systemu przed usunięciem śladów ingerencji osoby niepowołanej,
      IV. na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,

V. przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do systemu osoby niepowołanej,
VI. przywrócić normalny stan działania systemu.

3. Po wyeliminowaniu bezpośredniego zagrożenia ASI ma obowiązek przeprowadzić analizę stanu systemu informatycznego, a w szczególności sprawdzić:
   a) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   b) zawartość zbioru danych osobowych,
   c) sposób działania programów,
   d) jakość komunikacji w sieci telekomunikacyjnej,
   e) obecność wirusów komputerowych.

ZASADY POSTĘPOWANIA W PRZYPADKU STWIERDZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 22

1. Pracownik, który zauważył niepokojące zdarzenie, które mogą spowodować zagrożenie bądź mogą być przyczyną naruszenia ochrony danych osobowych i bezpieczeństwa informacji, zobowiązany jest do natychmiastowego poinformowania bezpośredniego przełożonego, ASI, ABI lub ADO.
2. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż ADO, jest ona zobowiązana poinformować o tym fakcie ADO.
3. Naruszeniu ochrony danych osobowych mogą świadczyć symptomy występujące w następujących obszarach:
   a) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych, w szczególności do serwerowni oraz kas, gdzie przechowuje są nośniki kopii zapasowych,
   b) włamanie lub próby włamania do szafek, w których przechowywane są , w postaci elektronicznej lub papierowej , nośniki danych osobowych,
   c) kradzież komputera, w którym przechowywane są dane osobowe,
   d) rozkręcona obudowa komputera,
   e) ograniczone lub poszerzone w stosunku do normalnej sytuacji, uprawnienia użytkownika w strukturze aplikacji
   f) inny zakres lub różnice w zawartości zbioru danych osobowych dostępnych dla użytkownika (np. ich całkowity lub częściowy brak lub nadmiar),
   g) zagubienie bądź kradzież nośnika z zawartością danych osobowych.

§ 23

1. Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość naruszenia bezpieczeństwa danych osobowych, ABI we współpracy z ASI, jest zobowiązany do podjęcia następujących kroków:
   1. stwierdzenia czy rzeczywiście doszło do naruszenia ochrony danych osobowych, w tym:
      I. sprawdzenia okoliczności zdarzenia,
      II. wyjaśnienia jego przyczyn, w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,
   2. w przypadku, gdy doszło do naruszenia ochrony danych osobowych to:
      I. zebranie ewentualnych dowodów,
      II. zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,
      III. zabezpieczenia danych przetwarzanych w systemie informatycznym, oraz wszelkich danych pomocnych w późniejszej analizie
      IV. usunięcia skutków incydentu i przywrócenia pierwotnego stanu systemu informatycznego tj. stanu sprzed incydentu, polegające na:
         - ✓ przeprowadzeniu analizy spójności danych osobowych przetwarzanych w systemie,
         - ✓ ewentualnym odtworzeniu kopii zapasowych danych i plików konfiguracyjnych,
         - ✓ przeprowadzeniu analizy poprawności funkcjonowania systemu informatycznego,

- ✓ powtórnym zabezpieczeniu danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.

§ 24

System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

§ 25

ABI określa, na podstawie zebranych informacji, przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym Spółdzielni.

§ 26

ABI prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

1. imię i nazwisko osoby zgłaszającej incydent,
2. imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
3. datę zgłoszenia incydentu,
4. przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
5. wyniki przeprowadzonych działań,
6. podjęte akcje naprawcze i ich skuteczność.

§ 27

ABI odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

1. określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
2. określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,
3. określenia potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

ZASADY UDOSTĘPNIANIA DANYCH OSOBOWYCH

§ 28

1. Udostępnianie danych osobowych ze zbioru danych, osobom lub podmiotom uprawnionym do ich otrzymania odbywać się może na pisemny, umotywowany wniosek.
2. Decyzję o udostępnieniu danych osobowych podejmuje ADO.
3. Po otrzymaniu zgody od ADO, dane do udostępnienia przygotowuje pracownik Spółdzielni merytorycznie odpowiedzialny za ich przetwarzanie.

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 29

1. Aktualny opis sposobu przepływu danych pomiędzy poszczególnymi systemami znajduje się w „Instrukcji zarządzania systemem informatycznym w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile stanowiącym załącznik Nr 1 do niniejszej Polityki.

2. Informacje zamieszczone w Załączniku Nr 1 powinny być aktualizowane po wprowadzeniu istotnych zmian w strukturach baz danych i związanych z tym zmian w zakresie bądź sposobie wymiany informacji pomiędzy nimi.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 30

Zasady ogólne

1. Zdając sobie sprawę iż żadne rozwiązania techniczne nie gwarantują pełnego bezpieczeństwa danych, konieczne jest, aby każdy użytkownik był świadom odpowiedzialności, i postępował zgodnie z przyjętymi w niniejszym dokumencie zasadami, ograniczając do minimum zagrożenia wynikające z błędów ludzkich.
2. Ochrona danych osobowych przetwarzanych w Spółdzielni obowiązuje wszystkie osoby, bez względu na zajmowane stanowisko oraz miejsce wykonywania, jak również charakter stosunku pracy.
3. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
4. Przetwarzać dane osobowe w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych otrzymane od ADO.
5. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
6. Identyfikator w sposób jednoznaczny identyfikuje danego użytkownika. Użytkownik ponosi odpowiedzialność za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
7. Po ustaniu stosunku pracy identyfikator danego użytkownika nie może zostać ponownie użyty w stosunku do żadnego innego użytkownika.
8. Wprowadzenie identyfikatora i hasła powinno odbywać się w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
9. Zachowanie tajemnicy służbowej obowiązuje pracownika zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
10. ABI i ADO jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur w całym systemie Spółdzielni.

§ 31

Środki organizacyjne

1. Wprowadzenie Polityki bezpieczeństwa w zakresie przetwarzania i ochrony danych osobowych oraz Instrukcji zarządzania systemem informatycznym .
2. Powołanie ADO, ABI i ASI odpowiedzialnych za działania organizacyjne i środki techniczne zapewniające odpowiedni poziom bezpieczeństwa danych osobowych.
3. Prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.
4. Kontrola dostępu do pomieszczeń, w których przetwarzane są dane osobowe oraz ścisła kontrola dostępu do pomieszczeń, w których znajdują się serwery.

§ 32

Środki techniczne

1. Poszczególne pomieszczenia, w których odbywa się przetwarzanie danych i ich składowanie wyposażono w drzwi z niezależnymi zamkami, które są zamykane podczas nieobecności pracowników. Po zakończeniu pracy osoba zamykająca pomieszczenie powinna dodatkowo sprawdzić czy zostały w nim zamknięte wszystkie okna i wyłączone wszystkie komputery.
2. Stanowiska komputerowe w pomieszczeniach, gdzie mogą czasowo przebywać osoby nieupoważnione do przetwarzania danych osobowych, powinny być tak usytuowane, aby uniemożliwić takim osobom wgląd w przetwarzane dane zarówno na monitorach jak i wydrukach.
3. Zbędne lub nieaktualne dokumenty powinny być bezwzględnie niszczone w niszczarkach.

Środki informatyczne

1. Ustalenie i przestrzeganie polityki dostępu do komputerów i programów przetwarzających dane za pomocą identyfikatorów i haseł.
2. Zgodne z „Instrukcją zarządzania systemem informatycznym" tworzenie kopii danych .
3. Ustalenie polityki ochrony antywirusowej.
4. Ustalenie polityki aktualizacji systemów operacyjnych pracujących na wszystkich komputerach Spółdzielni.
5. Utworzenie harmonogramu sprawdzania aktualizacji systemów i programów na stacjach roboczych.
6. W przypadku dłuższej bezczynności w pracy stanowiska komputerowego, automatycznie powinien uruchomić się wygaszacz ekranu chroniony hasłem lub użytkownik powinien sam zablokować stację tak, aby jej ponowne użycie było możliwe po podaniu hasła dostępu.
7. Serwer przetwarzający dane osobowe w zbiorze danych jest zabezpieczony zasilaczem awaryjnym z oprogramowaniem do automatycznego wyłączenia i restartu serwera w przypadku przekroczenia czasu podtrzymania zasilania z automatycznym, bezpiecznym wyłączeniem bazy danych osobowych.
8. Uprawnionym do przebywania w pomieszczeniu serwera jest wyłącznie ASI lub inne upoważnione osoby przy jego obecności. .
9. Krosowań lub zmian krosowań może dokonywać wyłącznie administrator sieci.

SPOSÓB POSTĘPOWANIA W ZAKRESIE KOMUNIKACJI POZA SIECIĄ LOKALNĄ

§ 33

Przy przesyłaniu danych osobowych poza siecią lokalną Spółdzielni wymagane jest zastosowanie szczególnych wymagań w zakresie bezpieczeństwa. Obejmują one:

1. Upoważnienia ADO.

2. Zastosowanie mechanizmów szyfrowania danych osobowych

    - przy szyfrowaniu symetrycznym algorytm AES z kluczem 256 bitów,
    - przy szyfrowaniu asymetrycznym algorytm RSA z kluczem 1024 bity,
    - funkcję skrótu SHA-1.

§ 34

W wypadku, gdy podmiot zewnętrzny, z którym wymieniane są dane osobowe, korzysta z innych mechanizmów kryptograficznych niż stosowane w Spółdzielni, możliwe jest zastosowanie tych mechanizmów lub mechanizmów z nimi zgodnych pod warunkiem zapewnienia zbliżonej do obowiązującej ochrony przesyłanych danych osobowych.

§ 35

W przypadku wystąpienia uzasadnionego podejrzenia przechwycenia kluczy kryptograficznych lub dostania się ich w niepowołane ręce pracownik zobowiązany jest poinformować o tym fakcie osoby uprawnione.