POLITYKA BEZPIECZEŃSTWA INFORMACJI

W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

w

Przychodni Promocji Zdrowia MEDICAMONITOR W LEGIONOWIE

ul. Reymonta 5

LEGIONOWO 2018

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE

Polityka Bezpieczeństwa, to dokument, który ma obowiązek opracować i wdrożyć każdy Administrator Danych Osobowych. Obowiązek posiadania Polityki Bezpieczeństwa, a także opis jej „konstrukcji" są przewidziane w następujących przepisach:

- Rozporządzeniu 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 /Dz. Urz. UE.L nr 119, str.1/,

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (U. 1997 nr 133 poz. 883), dalej: uodo,
- 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 (U. 2004 nr 100 poz. 1024), dalej: Rozporządzenie w sprawie dokumentacji,
- 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)

§1.

Celem Polityki Bezpieczeństwa Danych Osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w

zakresie ochrony danych osobowych, sposobu przetwarzania w Przychodni Promocji Zdrowia MEDICAMONITOR w Legionowie ,grupy informacji zawierającej dane osobowe.

§2.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. Jednostka – Przychodnia Promocji Zdrowia MEDICAMONITOR w Legionowie, ul. Reymonta 5
2. dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. przetwarzanie danych osobowych – gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
4. użytkownik – osoba upoważniona do przetwarzania danych osobowych,
5. administrator systemu – osoba upoważniona do zarządzania systemem informatycznym,
6. system informatyczny – system przetwarzania danych w Przychodni Promocji Zdrowia MEDICAMONITOR w Legionowie wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
7. zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§3.

1. Utrzymanie bezpieczeństwa przetwarzanych przez Jednostkę informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.
2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
   1) Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
   2) Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   3) Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   4) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.
3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) Niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
   2) Niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
   3) Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES

§4.

1. W systemie informacyjnym Jednostki przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.

2. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

§5.

Politykę Bezpieczeństwa stosuje się do:

1. danych osobowych przetwarzanych w systemie informatycznym,
2. wszystkich informacji dotyczących danych pracowników Jednostki, w tym danych osobowych personelu i treści zawieranych umów o pracę,
3. wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób dopuszczonych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§6.

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Jednostki w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§7.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

§8.

1. Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z:
   1) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
   2) Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w Jednostce - załącznik nr 1,
   3) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia- załącznik nr 2.

1. DOSTĘP DO INFORMACJI

§9.

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Jednostce zasad ochrony danych osobowych.

§10.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§11.

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, może być zrealizowane jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

§12.

Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§13.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

2. ZARZĄDZANIE DANYMI OSOBOWYMI

§14.

Administratorem danych osobowych Właściciele Przychodni Promocji Zdrowia MEDICAMONITOR w Legionowie

§15.

1. Za bezpieczeństwo danych osobowych Jednostki, odpowiadają:
    1) Administrator danych osobowych – Właściciele Przychodni

2) Administrator Bezpieczeństwa Informacji Jednostki – Właściciel Przychodni wskazany przez MEDICAMONITOR S.C. ,posiadający certyfikat przeszkolenia z tego zakresu.

2. Administrator Bezpieczeństwa Informacji Jednostki realizując politykę bezpieczeństwa informacji ma prawo wydawać instrukcje regulujące kwestie związane z ochroną danych w strukturach Jednostki.

3. W umowach zawieranych przez Jednostkę winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez Jednostkę.

§16.

1. Zapoznanie się z dokumentami określonymi w §8 pkt 2 pracownicy Jednostki potwierdzają podpisem na „Indywidualnym zakresie czynności osoby zatrudnionej przy przetwarzaniu danych osobowych" (wzór w załączniku nr 3) i przekazują Administratorowi Bezpieczeństwa Informacji.

§17.

Ochrona zasobów danych osobowych Jednostki jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników Jednostki.

3. ZAKRESY ODPOWIEDZIALNOŚCI

§18.

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Jednostki.

§19.

Administrator bezpieczeństwa informacji w Jednostce:

1. odpowiada za realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji,

2. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
3. określa strategię zabezpieczania systemów informatycznych Jednostki,
4. sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
5. sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
6. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Jednostki,
7. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
8. sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach, w których przetwarzane są dane osobowe,
9. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe,
10. monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
11. sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
12. zatwierdza wnioski o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
13. powiadamia administratora systemu o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
14. prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
15. prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych,
16. prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych,
17. prowadzi rejestr zbiorów danych osobowych Jednostki (przetwarzanych metodą tradycyjną lub w systemach informatycznych).

§20.

Administrator danych osobowych zobowiązany jest do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1. określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
2. określenie budynków, pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
3. zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
4. wykonywania zaleceń Administratora Bezpieczeństwa Informacji Jednostki w zakresie ochrony danych osobowych,
5. wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,
6. wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
7. działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
8. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,
9. odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
10. określanie, które osoby i na jakich prawach mają dostęp do danych informacji,

Praca Administratora Danych Osobowych jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

§21.

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
5. konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,

7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10. przyznawanie na wniosek Administratora Danych, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie,
11. wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
12. zarządzanie licencjami, procedurami ich dotyczącymi,
13. prowadzenie profilaktyki antywirusowej.

Praca Administratora Systemu Informatycznego jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

4. PRZETWARZANIE DANYCH OSOBOWYCH

§22.

1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach zamykanych na klucz przez wyznaczone do tego celu osoby.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§23.

1. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

5. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI PRZETWARZANYCH DANYCH

§24.

W Jednostce rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   - pomieszczenia zamykane na klucz,
   - szafy metalowe z zamkami,
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   - przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   - przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia organizacyjne:
   - osobą odpowiedzialną za bezpieczeństwo danych jest Administrator Bezpieczeństwa Informacji (ABI),
   - Administrator Bezpieczeństwa Informacji i wszyscy powołani przez niego administratorzy na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami,
4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
   - wykaz pracowników Jednostki uprawnionych do przetwarzania danych osobowych, znajduje się u Administratora Bezpieczeństwa Informacji- zał. nr 6
   - przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez Administratora Danych Osobowych- zał. Nr 5,
   - w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
   - przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,

– w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
– po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

6. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§25.

Archiwizacja informacji zawierających dane osobowe odbywa w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w wydzielonych pomieszczeniach, które są zabezpieczone przed dostępem osób nieupoważnionych (wykaz pomieszczeń załącznik nr 4)

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

w

Przychodni Promocji Zdrowia MEDICAMONITOR

w Legionowie, ul. Reymonta 5

§1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych.

§2

Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

1. stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§3

Każdy pracownik Jednostki, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) zobowiązany jest do niezwłocznego poinformowania o tym administratora tego systemu informatycznego lub w przypadku jego nieobecności administratora bezpieczeństwa informacji Jednostki.

§4

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§5

1. Administrator bazy danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:

1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,

2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,

3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.

4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.

   a) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,

   b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,

   c) zmianę hasła na konto administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.

5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

2. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

3. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.

4. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

5. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

§6

1. Administrator bazy danych osobowych, w której nastąpiło naruszenie ochrony danych osobowych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia przekazuje i administratorowi bezpieczeństwa informacji Jednostce.

2. Administrator bezpieczeństwa informacji w Jednostce przeprowadza analizę raportów i uwzględnia je w opracowywaniu corocznego raportu dla administratora danych w Jednostce.

WYKAZ POMIESZCZEŃ, W KTÓRYCH SĄ PRZETWARZANE, PRZECHOWYWANE, NISZCZONE DANE OSOBOWE W PRZYCHODNI PROMOCJI ZDROWIA MEDICAMONITOR w Legionowie, ul. Reymonta 5

pomieszczenia znajdujące się w budynku Jednostki przy ul. Reymonta 5 w Legionowie:

- recepcja

-gabinet medycyny pracy z zapleczem

-gabinet laryngologiczny i neurologiczny

-gabinet okulistyczny

-pokój pobrań do badań i punkt szczepień

-archiwum / w pomieszczeniach piwnicznych nr 1,2 i 3/

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji
w zakresie przetwarzania danych osobowych w Przychodni Promocji Zdrowia MEDICAMONITOR w Legionowie

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

w

PRZYCHODNI PROMOCJI ZDROWIA MEDICAMONITOR W LEGIONOWIE

ul. Reymonta 5

I. ZAKRES STOSOWANIA

Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, a w szczególności: sposób rejestrowania i wyrejestrowania użytkownika, sposób przydziału haseł i zasady korzystania z nich, procedury rozpoczęcia i zakończenie pracy, obowiązki użytkownika, metodę i częstotliwość tworzenia kopii, zasady sprawdzania obecności wirusów komputerowych oraz dokonywania przeglądów i konserwacji systemu.

II. OBSZAR PRZETWARZANIA DANYCH

1. Obszar przetwarzania danych osobowych z użyciem stacjonarnego sprzętu komputerowego stanowią pomieszczenia wykazane w załączniku nr 4.
2. Wszystkie pomieszczenia, które należą do obszaru przetwarzania danych, wyposażone są w zamknięcia. W czasie, gdy nie znajdują się w nich osoby upoważnione, pomieszczenia są zamykane w sposób uniemożliwiający wstęp osobom nieupoważnionym. Osoby nieupoważnione mogą przebywać w obszarze przetwarzania danych tylko za zgodą Administratora Danych lub w obecności osób upoważnionych.

III. REJESTROWANIE I WYREJESTROWANIE UŻYTKOWNIKA

1. Użytkownikiem systemu informatycznego (osobą upoważnioną) może być:
   a) osoba zatrudniona przy przetwarzaniu danych osobowych w Jednostce, która posiada upoważnienie do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład,
   b) pracownik innego podmiotu lub przedsiębiorca będący osobą fizyczną prowadzi działalność na podstawie wpisu do ewidencji działalności gospodarczej, którzy świadczą na podstawie stosowanych umów usługi związane z ich pracą w systemie informatycznym (serwis, zlecenie przetwarzania danych osobowych itp.).

2. Uzyskanie uprawnień następuje na dwóch poziomach:

a) zarejestrowania w sieci komputerowej (założenie konta),
b) nadanie określonych uprawnień do korzystania z systemu komputerowego.

3. Pisemny wniosek o zarejestrowanie użytkownika składa bezpośredni przełożony pracownika. Wniosek zostaje przekazany do Administratora Bezpieczeństwa Informacji, który może zgłosić sprzeciw wobec przyznania uprawnień, ze względu na zagrożenie naruszenia bezpieczeństwa danych osobowych.

4. W przypadku zakończenia pracy w Jednostce, stosuje się następująca procedurę wyrejestrowania użytkownika:
   1) na karcie obiegowej, na której osoba odchodząca zbiera podpisy potwierdzenia rozliczenia się z pracodawcą, znajduje się pozycja stwierdzająca fakt usunięcia lub zablokowania profilu użytkownika,
   2) Administrator Bezpieczeństwa Informacji jako osoba upoważniona do podpisania obiegówki przed podpisaniem pozycji stwierdzającej fakt usunięcia lub zablokowania profilu użytkownika wydaje polecenie administratorowi systemu o natychmiastowym wykonaniu tej czynności,
   3) po wykonaniu tej czynności następuje podpisanie przez Administratora Bezpieczeństwa Informacji obiegówki potwierdzającej usunięcie lub zablokowanie profilu użytkownika,
   4) wykonanie tej operacji jest jednoznaczne z uniemożliwieniem dostępu do systemu dla pracownika, z którym rozwiązano umowę o pracę w Jednostce,

IV. SPOSÓB PRZYDZIAŁU HASEŁ I ZASADY KORZYSTANIA Z NICH

1. Każdorazowe uwierzytelnienie użytkownika w systemie następuje po podaniu loginu i hasła.
2. Używanie hasła jest obowiązkowe dla każdego użytkownika, posiadającego login w systemie.
3. W Jednostce obowiązują następujące zasady korzystania z haseł:
   a) zabrania się ujawniania haseł jakimkolwiek osobom trzecim,
   b) zabrania się zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim.

4. Prawidłowe wykonywanie obowiązków związanych z korzystaniem użytkowników z haseł nadzoruje Administrator Bezpieczeństwa Informacji. Nadzór ten w

szczególności polega na obserwacji (monitorowaniu) funkcjonowania mechanizmu uwierzytelniania i przywracania stanu prawidłowego w przypadku nieprawidłowości.

V. ROZPOCZĘCIE I ZAKOŃCZENIE PRACY

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych. W przypadku naruszenia ochrony danych osobowych użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   a) włączenia komputera,
   b) uwierzytelnienia się („zalogowania" w systemie) za pomocą loginu i hasła.
3. Niedopuszczalne jest uwierzytelnianie się na hasło i login innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.
4. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dyskietki, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.
5. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się" lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania" się do systemu.
6. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się" w systemie), użytkownik niezwłocznie powiadamia o nich administratora.

VI. TWORZENIE, PRZECHOWYWANIE, SPRAWDZANIE PRZYDATNOŚCI I LIKWIDACJI KOPII ZAPASOWYCH

1. Kopie zapasowe są tworzone, przechowywane i wykorzystywane z uwzględnieniem następujących zasad:
   a) kopie wykonywane są co miesiąc na płytach CD/DVD lub innych nośnikach danych

b) kopie są okresowo, raz w miesiącu, sprawdzane pod kątem ich przydatności do odtworzenia danych, a jeżeli ustanie ich użyteczność są niezwłocznie usuwane.

VII. SPRAWDZANIE OBECNOŚCI WIRUSÓW KOMPUTEROWYCH

1. Sprawdzanie obecności wirusów komputerowych dokonywane jest poprzez zainstalowanie programu, który skanuje automatycznie, bez udziału użytkownika, na obecność wirusów wszystkie pliki. Program jest zainstalowany na wszystkich stacjach roboczych.
2. Po każdej naprawie i konserwacji komputera należy dokonać sprawdzenia pod kątem występowania wirusów i ponownie zainstalować program antywirusowy.
3. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich. Dane uzyskiwane drogą teletransmisji należy umieszczać – przed otwarciem – w katalogu przejściowym, który podlega sprawdzeniu.

VIII. SPOSÓB I CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI, W TYM KOPII INFORMATYCZNYCH I WYDRUKÓW

1. Wydruki i dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w odrębnych zamykanych szafach.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych sporządzająca wydruk zawierający dane osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności – niezwłocznie wydruk zniszczyć.
3. Elektroniczne nośniki informacji z danymi osobowymi są oznaczane i przechowywane w zamykanych szafach lub sejfach znajdujących się w specjalnym pomieszczeniu, do którego dostęp mają wyłącznie odrębnie upoważnieni pracownicy.
4. Fizyczna likwidacja zniszczonych lub niepotrzebnych elektronicznych nośników informacji z danymi osobowymi odbywa się w sposób uniemożliwiający odczyt danych osobowych.
5. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania

danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

IX. ZASADY PRZEGLĄDANIA I KONSERWACJI SYSTEMU

1. Przegląd i konserwacja zbiorów danych dokonywane są poprzez:
    a) badanie spójności bazy danych,
    b) uruchamianie zapytań do bazy danych w celu analizy danych,
    c) przegląd wydruków po wyznaczonych procesach,
    d) sprawdzanie zgodności danych z dokumentami,
    e) analiza zgłaszanych uwag użytkowników.

2. Przeglądu i konserwacji dokonują specjalista ds Informatyki w porozumieniu z Administratorem Bezpieczeństwa Informacji.

3. W przypadku zlecenia wykonywania czynności, o których mowa wyżej, podmiotowi zewnętrznemu, wszelkie prace powinny odbywać się pod nadzorem Administratora Bezpieczeństwa Informacji.

X. KOMUNIKACJA W SIECI KOMPUTEROWEJ

1. W zakresie korzystania z sieci komputerowej w Jednostce obowiązują następujące zasady:
    a) pracownicy nie są uprawnieni do instalacji jakiegokolwiek prywatnego oprogramowania. W przypadku zainstalowania takiego oprogramowania bez odpowiedniej akceptacji pracownik ponosi odpowiedzialność porządkową i prawną,
    b) oprogramowanie na komputerach może być zainstalowane wyłącznie przez informatyka,
    c) pracownicy nie mają prawa przekazywać za pośrednictwem sieci komputerowej do stron trzecich jakichkolwiek danych stanowiących własność Jednostki,
    d) pracownicy nie mogą ściągać za pośrednictwem sieci komputerowej żadnego oprogramowania,

XI. OBOWIĄZKI I ODPOWIEDZILANOŚĆ UŻYTKOWNIKA ZWIĄZANE Z OBOWIĄZYWANIEM INSTRUKCJI

1. Użytkownik systemu jest zobowiązany zapoznać się z treścią niniejszej Instrukcji i potwierdzić to stosownym oświadczeniem.
2. Naruszenie przez pracownika niniejszej Instrukcji może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu pracy odpowiedzialność pracownika.
3. Treść niniejszej Instrukcji ma charakter poufny, chroniony tajemnicą pracodawcy na zasadzie art. 100 § 2 pkt 4 Kodeksu pracy.

Legionowo, dnia .....

Upoważnienie imienne

do przetwarzania danych osobowych

Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) upoważniam Panią / Pana:

.....

(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w

.....

(nazwa jednostki i komórki organizacyjnej)

na

stanowisku: .....
.....

do przetwarzania od dnia ..... r. danych osobowych w

zakresie : .....
.....

i nadaję

identyfikator: .....

.....

(podpis administratora danych)

Legionowo, dnia .....

OŚWIADCZENIE

Oświadczam, że przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/ny z przepisami dotyczącymi ochrony danych osobowych, w tym z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z poźn. zm.) oraz rozporządzeniami wykonawczymi wydanymi na jej podstawie.

Zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w:

- Polityce bezpieczeństwa przetwarzania danych osobowych w Przychodni Promocji Zdrowia MEDICAMONITOR w Legionowie
- Instrukcji zarządzania systemem informatycznym w Przychodni Promocji Zdrowia MEDICAMONITOR w Legionowie
- Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Przychodni Promocji Zdrowia MEDICAMONITOR w Legionowie

.....
podpis pracownika