POLITYKA BEZPIECZEŃSTWA INFORMACJI I INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W PRZYCHODNI MEDYCYNY RODZINNEJ VIOLETTA ŻYLIŃSKA Z SIEDZIBĄ W WOLI UHRUSKIEJ UL. 1 MAJA 1, 22-230 WOLA UHRUSKA

SPIS TREŚCI

ROZDZIAŁ I
WSTĘP

Niniejsza polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i ws prawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1), oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

Administrator Danych, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń danych osobowych przetwarzanych w związku z wykonywaniem zadań Administratora Danych, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom, m. in. takim jak:

1. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej;
2. niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura);
3. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą Administratora Danych;
4. podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;
5. celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego Administratora Danych;
6. ataki z Internetu;
7. naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:
   a) niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu),
   b) naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   c) ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u Administratora Danych,
   d) ujawnienie osobom nieupoważnionym danych przetwarzanych przez Administratora Danych,
   w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach Administratora Danych,
   e) przetwarzanie danych osobowych w celach prywatnych,
   f) wprowadzanie zmian do systemu informatycznego Administratora Danych i instalowanie programów bez zgody IOD lub Administratora Danych.

ROZDZIAŁ II
POSTANOWIENIA OGÓLNE
§ 1

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Administratorze Danych (AD)** rozumie się przez to Przychodnia Medycyny Rodzinnej Violetta Żylińska z siedzibą w Woli Uhruskiej, w rozumieniu art. 4 pkt 7 Rozporządzenia.
2. **Inspektor Ochrony Danych Osobowych (IOD)** rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych w przypadkach i na zasadach określonych w art. 37 rozporządzenia.
3. **Danych osobowych** na podstawie Art. 4 pkt 1 Rozporządzenia dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

4. **Identyfikatorze użytkownika** rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
5. **Integralności danych** rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostaną przypadkiem ani celowo zmienione lub uszkodzone.
6. **Odbiorcy danych** na podstawie art. 4 pkt 9 Rozporządzenia odbiorca oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby upoważnionej do przetwarzania danych osobowych,
   e) organów państwowych lub organów samorządu terytorialnego, NFZ, którym dane są udostępniane w związku z prowadzonym postępowaniem.
7. **Osobie upoważnionej do przetwarzania danych osobowych** rozumie się przez to osobę, która została upoważniona do przetwarzania danych osobowych przez Administratora Danych - na piśmie.
8. **Poufności danych** rozumie się przez to właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobą i podmiotom.
9. **Przetwarzającym** rozumie się przez to osobę fizyczną lub prawną organ publiczny lub inny podmiot, który przetwarza dane osobowe w imieniu administratora w rozumieniu art. 4 pkt 8 Rozporządzenia.
10. **Przetwarzaniu danych** rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany taką jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
11. **Raporcie** rozumie się przez to przygotowane przez System informatyczny zestawienia zakresu i treści przetwarzanych danych osobowych.
12. **Rozliczności** rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi w rozumieniu art. 5 ust 2 Rozporządzenia.
13. **Sieci publicznej** rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt.28 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2017 r. poz. 1907 ze zm.)
14. **Sieci teleinformatycznej** rozumie się przez to służącą do przetwarzania danych osobowych organizacyjnie i technicznie połączenie systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami.
15. **Sieci telekomunikacyjnej** rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt.35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2017 r. poz. 1907 ze zm.).
16. **Serwisancie** rozumie się przez to firmę lub pracownika firmy zajmującego się aktualizacją lub instalacją oprogramowania.
17. **Systemie Informatycznym Administratora Danych** rozumie się przez sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje przynajmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną.
18. **Przychodnia** rozumie się przez to Przychodnię Medycyny Rodzinnej Violetta Żylińska z siedzibą w Woli Uhruskiej.
19. **Teletransmisji (zdalnego połączenia)** rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej, zdalnego połączenia z komputerem w celu np. naprawy błędu programu.
20. **Rozporządzeniu** rozumie się przez to rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 27.04.2016 r.
21. **Ustawie** rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych.
22. **Usuwaniu danych** rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
23. **Uwierzytelnianiu** rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu lub osoby upoważnionej do przetwarzania danych osobowych.
24. **Użytkowniku** rozumie się przez to osobę upoważnioną do dostępu i przetwarzania danych osobowych, której nadano Identyfikator użytkownika i przyznano hasło.
25. **Zabezpieczeniu danych w systemie informatycznym** rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

26. **Zabezpieczeniu systemu informatycznego** rozumie się przez to wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
27. **Zbiorze danych** rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

§ 2

1. Polityka Bezpieczeństwa i Instrukcja zarządzania systemem informatycznym to zbiór działań, zmierzających do uzyskania i utrzymania wymaganego poziomu bezpieczeństwa danych osobowych, tj. zapewnienie poufności, integralności, spójności, odpowiedniości i dostępności na każdym etapie tworzenia, przetwarzania, przechowywania i przesyłania danych osobowych.
2. W związku z tym, że w zbiorach Administratora Danych przetwarzane są między innymi dane wrażliwe, (m. in. informacje dotyczące stanu zdrowia oraz inne) a system informatyczny Administratora Danych posiada połączenie z Internetem, niniejszy dokument służy zapewnieniu **wysokiego poziomu bezpieczeństwa danych**.
3. Polityka Bezpieczeństwa i Instrukcja zarządzania systemem informatycznym obejmuje zbiór zasad dotyczących bezpieczeństwa danych osobowych ustalonych w oparciu o wymagania wynikające z przepisów prawa, z szacowania ryzyka w związku z wykonywaniem określonych prawem zadań przez Przychodnię oraz wewnętrzne wymogi i uwarunkowania lokalowe.
4. Polityka Bezpieczeństwa i Instrukcja zarządzania systemem informatycznym zapewnia:
   a) spójność z wyznaczonymi zadaniami Przychodni oraz pełną integrację z podstawowymi procedurami zdefiniowanymi w Przychodni,
   b) skuteczniejsze działania w odniesieniu do zagrożeń poufności, integralności i dostępności danych osobowych, realizację zadań Przychodni w taki sposób, aby podnieść jakość i wiarygodność wobec pacjentów oraz petentów,
   c) ochronę danych osobowych tworzonych, przetwarzanych, przechowywanych i przesyłanych nie tylko za pomocą systemów informatycznych ale również w innych obszarach ich przetwarzania i przechowywania (np. w wersji papierowej).
5. Celem Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym jest wskazanie działań, jakie należy podejmować oraz ustanowienie zasad, jakie należy stosować, aby prawidłowo były realizowane obowiązki Przychodni jako Administratora Danych w zakresie zabezpieczenia danych osobowych.
6. Niniejszy dokument dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.
7. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych w Przychodni, jak i innych, np. stażystów, praktykantów, osób zatrudnionych na umowę zlecenie.

§ 3

Z uwagi na fakt, że w Przychodni urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączone są z siecią publiczną (Internet), stosuje się wysoki poziom bezpieczeństwa teleinformatycznego.

§ 4

Bezpieczeństwo teleinformatyczne na poziomie wysokim zapewnia się przez:

1. ochronę fizyczną,
2. ochronę antywirusową,
3. bezpieczeństwo teletransmisji (połączenia zdalnego),
4. kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej.

§ 5

Ochronę fizyczną systemu lub sieci teleinformatycznej zapewnia się przez instalację środków zabezpieczających pomieszczenia, w którym znajdują się urządzenia systemu lub sieci teleinformatycznej, w szczególności przed:

1. nieuprawnionym dostępem,
2. podglądem.

§ 6

Ochrona antywirusowa systemu operacyjnego lub sieci komputerowej polega na stosowaniu oprogramowania antywirusowego.

ROZDZIAŁ III
ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

§ 7

Administrator Danych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków,
2. wyznacza Inspektora Ochrony Danych Osobowych oraz określa zakres jego zadań i czynności,
3. prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych, o ile jako właściwy do jej prowadzenia nie zostanie wskazany w niniejszym dokumencie inny podmiot,
4. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.
5. prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
6. przetwarza dane osobowe zgodnie z zasadami określonymi w art. 5 Rozporządzenia,
7. przetwarza dane na jednej z podstaw określonych w art. 6 lub art. 9 Rozporządzenia
8. zapewnia bezpieczeństwo danych zgodnie z art. 24 i 32 Rozporządzenia
9. współpracuje z organem nadzorczym,
10. zapewnia stopień bezpieczeństwa danych odpowiadający ryzyku naruszenia praw lub wolności osób, których dane przetwarza z godnie z art. 32 Rozporządzenia,
11. zgłasza organowi nadzorczemu naruszenie ochrony danych osobowych zgodnie z art. 33 Rozporządzenia,
12. zawiadamia osoby, których dane zostały dotknięte naruszeniem ochrony danych zgodnie z art. 34 Rozporządzenia.

§ 8

Inspektor Ochrony Danych Osobowych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1. sprawuje nadzór nad zastosowaniem środków technicznych, a także organizacyjnych w celu zapewnienia bezpieczeństwa danych,
2. nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
3. realizuje obowiązek informacyjny,
4. monitoruje przestrzeganie przepisów Rozporządzenia oraz Ustawy poprzez:
   a) zbieranie informacji w celu identyfikacji procesów przetwarzania,
   b) analizowanie i sprawdzanie zgodności tego przetwarzania,
   c) informowanie, doradzanie i rekomendowanie określonych działań Administratorowi Danych.
5. współpracuje z organem nadzorczym, w tym pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.

§ 9

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1. Może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy bądź odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.
2. Musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora Danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.

3. Zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
4. Stosuje określone przez Administratora Danych oraz Inspektora Ochrony Danych Osobowych procedury oraz wytyczne mające na celu przetwarzanie danych osobowych zgodnie z Rozporządzenie oraz Ustawą.
5. Korzysta z systemu informatycznego Administratora Danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników.
6. Zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

ROZDZIAŁ IV
WYKAZ POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE
§ 10

1. Budynkiem, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest budynek Przychodni Medycy Rodzinnej Violetta Żylińska w Woli Uhruskiej mieszczący się pod adresem: ul. 1 Maja 1, 22-230 Wola Uhruska.
2. Pomieszczeniami tworzącymi obszar, w którym znajdują się przetwarzane dane osobowe są pomieszczenia, w których znajdują się zbiory danych w formie kartotek, rejestrów i innej oraz stacjonarny sprzęt komputerowy, w którym są przetwarzane dane osobowe.
3. Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru, o którym mowa w ust. 2, osób nieuprawnionych do dostępu do danych osobowych, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych, Administratora Danych lub Inspektora Ochrony Danych Osobowych.
4. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na klucz i chronione na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osób trzecich.
5. Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe został określony w załączniku nr 1 do niniejszej Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

ROZDZIAŁ V
WYKAZ ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMY ZASTOSOWANE DO PRZETWARZANIA TYCH DANYCH
§ 11

Wykaz zbiorów danych osobowych oraz programów zastosowanych do przetwarzania tych danych zawiera **załącznik nr 2** do Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

ROZDZIAŁ VI
OPIS STRUKTURY ZBIORÓW DANYCH
§ 12

Opis zbiorów danych zawiera **załącznik nr 3** do Polityki Bezpieczeństwa Instrukcji Zarządzania Systemem Informatycznym.

Rozdział VII
ZASADY ROZPOCZĘCIA, ZAWIESZENIA i ZAKOŃCZENIA PRACY SYSTEMU INFORMATYCZNEGO

1. Przed przystąpieniem do pracy w systemie informatycznym należy:
   a) sprawdzić stanowisko pracy, a następnie włączyć zasilacz UPS/listwę zasilającą;
   b) włączyć monitor oraz wszystkie urządzenia peryferyjne: skaner, drukarka itd;
   c) włączyć komputer;
   d) zalogować się do systemu operacyjnego używając odpowiedniego identyfikatora (loginu) oraz hasła;
   e) bezwzględnie należy zapewnić zachowanie poufności podczas wprowadzania hasła, niedopuszczalnym jest by osoba nieupoważniona do przetwarzania danych osobowych przyglądała się wprowadzaniu hasła;
   f) po uruchomieniu systemu operacyjnego można rozpocząć pracę na programie użytkowym;

2. Podczas nawet chwilowego opuszczenia stanowiska pracy należy zablokować możliwość wglądu do przetwarzanych danych przez osoby trzecie poprzez wylogowanie użytkownika z programu użytkowego /systemu operacyjnego używając odpowiedniego skrótu klawiszowego lub wybierając funkcję wyloguj w systemie operacyjnym;
3. Na czas dłuższej nieobecności (wyjścia z pomieszczenia) należy wyłączyć komputer.
4. W celu zakończenia pracy w systemie informatycznym należy:
   a) wylogować się z używanego programu użytkowego używając odpowiedniej opcji,
   b) dokonać zamknięcia systemu operacyjnego odpowiednią funkcją,
   c) odczekać aż system operacyjny zostanie wyłączony,
   d) wyłączyć zasilanie stanowiska komputerowego poprzez wyłączenie zasilacza UPS lub listwy zasilającej;

Rozdział VIII
ZASADY KORZYSTANIA Z KOMPUTERÓW PRZENOŚNYCH PRZY UŻYCIU KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

§ 13

Przetwarzanie danych osobowych przy użyciu komputerów przenośnych odbywać się może wyłącznie za wiedzą i zgodą Inspektora Ochrony Danych Osobowych.

§ 14

Osoba użytkująca komputer przenośny, w którym przetwarzane są dane osobowe, zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

§ 15

Użytkownik komputera przenośnego zobowiązany jest do:
1. Transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia,a w szczególności:
   a) transportowania komputera w bagażu podręcznym,
   b) niepozostawiania komputera w samochodzie, przechowalni bagażu itp.,
   c) przenoszenia komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych.
2. Korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzania danych osobowych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i środkach transportu publicznego.
3. Niezezwalania osobom nieupoważnionym **(w tym również członkom rodziny i znajomym)** do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym Administratora Danych.
4. Niepodłączenia komputera przenośnego do Internetu za wyjątkiem podłączeń do sieci informatycznej na stałym stanowisku pracy.
5. Zabezpieczenia komputera przenośnego hasłem.
6. Blokowanie komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez użytkownika komputera przenośnego, jak również stosowania innych mechanizmów zabezpieczających.
7. Program antywirusowy zainstalowany na komputerze przenośnym powinien być zaktualizowany do najnowszej wersji oraz posiadać najnowszą bazę wirusów. Użytkownik jest zobowiązany przynajmniej raz w tygodniu w pełni przeskanować komputer programem antywirusowym

§ 16

Użytkownicy komputerów przenośnych nie mogą, bez zgody Administratora Danych oraz Inspektora Ochrony Danych, instalować na użytkowanych przez siebie komputerach oprogramowania.

§ 17

W razie zagubienia lub kradzieży komputera przenośnego pracownik zobowiązany jest do natychmiastowego powiadomienia IOD lub osoby przez niego upoważnionej zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

§ 18

W sprawach nieuregulowanych w niniejszym rozdziale stosuje się odpowiednio przepisy dotyczące przetwarzania danych osobowych w systemach informatycznych na komputerach stacjonarnych.

ROZDZIAŁ IX
STRATEGIA ZABEZPIECZENIA DANYCH OSOBOWYCH (DZIAŁANIA NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH)

§ 19

1. Celem wprowadzonych niniejszą Polityką zabezpieczeń i obostrzeń jest ochrona danych osobowych zawartych w systemie eksploatowanym w sieci komputerowej.
2. Określone niżej sposoby zabezpieczeń dotyczą:
   a) zabezpieczeń przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemu tj. wprowadzanie danych, aktualizacji lub usuwania danych, wyświetlania lub drukowania zestawień, wypisów;
   b) ochrony danych zarchiwizowanych na nośnikach zewnętrznych, procedur niszczenia niepotrzebnych wydruków lub nośników danych,
   c) systemu zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia oraz sposobów dostępu do tych pomieszczeń pracowników, personelu pomocniczego oraz serwisu zewnętrznego,
   d) monitorowania systemu zabezpieczeń,
   e) zakresu obowiązków pracowników w części dotyczącej bezpieczeństwa danych.
3. Strategia ochrony danych osobowych opiera się na następujących zasadach:
   a) fizyczny dostęp do pomieszczeń, w których eksploatowane są systemy informatyczne blokują drzwi zamykane na klucz,
   b) podstawowym sposobem zabezpieczenia danych i dostępu do nich jest system definiowania użytkowników, grup użytkowników oraz haseł. Są to zabezpieczenia programowe wmontowane w eksploatowane systemy uniemożliwiające dostęp do systemu osobom nieupoważnionym,

§ 20

1. Należy chronić dokumenty papierowe zawierające dane osobowe przed ich fizycznym uszkodzeniem lub zniszczeniem, co uniemożliwiałoby odczytanie lub odzyskanie informacji w nich zawartych.
2. Dokumenty papierowe zawierające dane osobowe muszą być chronione przed zagrożeniami ze strony otoczenia (ogień, wyciek wody itp.).
3. Dokumenty papierowe powinny być fizycznie chronione przed kradzieżą, zniszczeniem lub niewłaściwym używaniem. Opuszczając stanowisko pracy należy sprawdzić czy są one zamknięte w odpowiednich szafach czy sejfach.
4. Zabrania się kopiowania jakichkolwiek danych osobowych zawartych na dokumentach papierowych bez zgody IOD lub osoby przez niego upoważnionej.
5. Usunięcie lub wyniesienie poza siedzibę Przychodni dokumentu papierowego zawierającego dane osobowe wymaga zgody IOD lub upoważnionej przez niego osoby.
6. Utrata i kradzież dokumentów papierowych zawierających dane osobowe powinna być niezwłocznie zgłoszona IOD.
7. Każdy dokument papierowy zawierający dane osobowe, mający charakter dokumentu roboczego, należy na koniec pracy zniszczyć w niszczarce papieru lub schować w odpowiedniej zamykanej szafie.

§ 21

1. Nośniki pamięci (płyty, pendrive, itp.) zawierające dane osobowe należy bezwzględnie zabezpieczyć przed ich kradzieżą, fizycznym uszkodzeniem lub zniszczeniem, co uniemożliwiłoby odczytanie lub odzyskanie informacji w nich zawartych. Każdy pendrive oraz dysk przenośny powinien być zaszyfrowany odpowiednim programem.
2. Nośniki pamięci zawierające dane osobowe należy bezwzględnie chronić przed zagrożeniami ze strony otoczenia (kurz, promieniowanie elektromagnetyczne, ogień, wyciek wody itp.).
3. Opuszczając stanowisko pracy należy sprawdzić czy są one zamknięte w odpowiednich szafach czy sejfach.
4. Zabrania się kopiowania jakichkolwiek zbiorów danych osobowych z nośników pamięci bez zgody IOD.

5. Nośniki pamięci zawierające dane osobowe nie mogą być wynoszone poza siedzibę Przychodni bez wcześniejszej zgody IOD.
6. Nośniki pamięci zawierające dane osobowe mogą być wynoszone poza teren Przychodni przez osoby upoważnione za zgodą Administratora Danych.
7. Dyski twarde komputerów przeznaczone do naprawy, pozbawia się przed naprawą zapisu danych osobowych albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora Danych.
8. Każdy nośnik pamięci przeznaczony do usunięcia z Przychodni musi uzyskać odpowiednie pozwolenie IOD.
9. Niszczenia zużytych lub uszkodzonych nośników pamięci zawierających dane osobowe dokonuje osoba upoważniona przez Administratora Danych.:
   a) płyty CD – należy zniszczyć w niszczarce dokumentów dostosowanej do niszczenia płyt CD lub zniszczyć przy pomocy ostrego narzędzia rysując powierzchnię przeznaczoną do zapisu,
   c) twarde dyski (HDD/SSD) – rozmontować urządzenie w celu odsłonięcia talerzy z zapisem magnetycznym, a następnie używając twardego i ostrego narzędzia zniszczyć powierzchnię dysku poprzez zarysowanie jej kilkudziesięcioma rysami, lub należy użyć młotka w celu zniszczenia talerzy magnetycznych i ceramicznych,
   d) pendrive – należy użyć młotka w celu uszkodzenia układów pamięci poprzez ich fizyczne zniszczenie.
10. Utrata lub kradzież nośnika pamięci z danymi osobowymi powinna być niezwłocznie zgłoszona Administratorowi Danych.

§ 22

1. Wprowadza się następujące zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym:
   a) na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się wysoki poziom zabezpieczeń,
   b) ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera, na których przetwarzane są dane osobowe zapewniają zasilacze UPS,
   c) zalogowanie się do programu wymaga podania nazwy użytkownika i hasła.
   d) oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień,
2. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe.
3. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
4. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.
5. Stosuje się następujące zabezpieczenia organizacyjne przed dostępem do danych osób niepowołanych:
   a) dostęp do danych mają wyłącznie pracownicy upoważnieni przez Administratora Danych,
   b) w pokoju rejestracji, do którego dostęp mają petenci monitory komputerowe ustawione są w ten sposób, by pacjenci nie widzieli zapisów na ekranie,
   c) w przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacie ekranu, których usunięcie jest możliwe po podaniu prawidłowego hasła użytkownika,

§ 23

1. Ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez zawieranie umów powierzenia przetwarzania danych osobowych.
2. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia administratora danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

§ 24

1. Urządzenia systemu informatycznego Administratora Danych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).
2. Bieżąca konserwacja sprzętu wykorzystywanego przez Administratora Danych do przetwarzania danych prowadzona jest tylko przez osoby upoważnionej przez Administratora Danych. Natomiast poważne naprawy wykonywane przez serwisantów realizowane są w siedzibie Administratora Danych po zawarciu

z podmiotem wykonującym naprawę umowy o powierzeniu przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.

3. Administrator dopuszcza konserwowanie i naprawę sprzętu poza siedzibą Administratora Danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy o powierzeniu przetwarzania danych.
4. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące, a także przez IOD.

§ 25

Dla zachowania bezpieczeństwa danych zobowiązuje się osoby upoważnione do przetwarzania danych lub Użytkowników do:

1. ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia,
2. niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu, komputerów przenośnych w hotelach i innych miejscach publicznych oraz w samochodach,
3. dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie),
4. niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory),
5. pilnego strzeżenia akt, dokumentacji medycznej; pamięci przenośnych i komputerów przenośnych,
6. kasowania po wykorzystaniu danych na dyskach przenośnych,
7. nieużywania powtórnie dokumentów zadrukowanych jednostronnie,
8. niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze (niedopuszczalnym jest zapisywania hasła w widocznym miejscu), w komputerze lub innym nośniku danych,
9. powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych,
10. przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń IOD,
11. opuszczania stanowiska pracy dopiero po włączeniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób,
12. kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane,
13. niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej,
14. wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie,
15. kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie,
16. niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy,
17. niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
18. zachowania tajemnicy danych, w tym także wobec najbliższych,
19. chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy,
20. umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy,
21. zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych,
22. zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,

23. zamykania drzwi na klucz po zakończeniu pracy w danym dniu.

§ 26

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do stosowania następujących zasad:

1. Dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego Administratora Danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone.
2. Nośniki pamięci przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazanie informacji oraz formatowanie nośnika.
3. Uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników (płyty CD/DVD).
4. Zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Po wykorzystaniu brudnopisu, należy go niezwłocznie zniszczyć w niszczarce.
5. W przypadku brudnopisów pism drukowanych dwustronnie należy je po wykorzystaniu niezwłocznie zniszczyć w niszczarce.
6. Po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę Administratora Danych.

§ 27

Zobowiązuje się osoby upoważnione do stosowania następujących zasad:

1. Wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów.
2. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.
3. Przed atakami z sieci zewnętrznej wszystkie komputery Administratora Danych (w tym także przenośne) chronione są środkami dobranymi przez Administratora Danych. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń – system operacyjny oraz program antywirusowy musi być AKTUALNY!

§ 28

1. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z programu komputerowego, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń IOD oraz Administratora Danych.

§ 29

1. Korzystanie z zasobów sieci wewnętrznej jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.
2. Operacje za pośrednictwem rachunku bankowego Administratora Danych może wykonywać wyłącznie pracownik wyznaczony, posiadający odpowiednie dane do uwierzytelnienia oraz konto w systemie, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

§ 30

1. Udostępnianie danych osobowych odbiorcom których dane dotyczą odbywa się na zasadach opisanych w art. 15 Rozporządzenia, przy czym pierwsza kopia danych osobowych podlegających przetwarzaniu powinna zostać udostępniona bezpłatnie.

2. Udostępnianie danych osobowych funkcjonariuszom Policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
   a) oznaczenie wnioskodawcy,
   b) wskazanie przepisów uprawniających do dostępu do informacji,
   c) określenie zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
   d) wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.
3. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.
4. Osoba udostępniająca dane osobowe jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.
5. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
6. Osoba upoważniona może udostępnić dane osobowe innym służbom i podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 31

1. Niezastosowanie się do prowadzonej przez Administratora Danych Polityki Bezpieczeństwa Informacji przetwarzania danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia z winy pracownika na podstawie art. 52 Kodeksu pracy (t.j. Dz.U. z 2018 r. poz. 917 ze zm.).
2. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 49-52 Ustawy oraz art. 266 Kodeksu Karnego (t.j. Dz.U. z 2017 r. poz. 2204 ze zm.).
3. Przykładowo przestępstwo można popełnić wskutek:
   a) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,
   b) niezabezpieczenia nośnika lub komputera przenośnego,
   c) zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym Administratora Danych.

ROZDZIAŁ X
ŚRODKI TECHNICZNE I ORGANIZACYJNE SŁUŻĄCE ZAPEWNIENIU POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

System informatyczny w Przychodni w Woli Uhruskiej ze względu na połączenie z siecią publiczną, musi zapewniać środki bezpieczeństwa określone dla wysokiego poziomu bezpieczeństwa.

§ 32

1. Gwarancją zapewnienia bezpieczeństwa systemu informatycznego oraz przetwarzanych i przechowywanych danych osobowych jest zapewnienie bezpieczeństwa fizycznego.
2. Obowiązkiem osoby użytkującej komputer przenośny zawierający dane osobowe jest zachowanie szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza pomieszczeniami tworzącymi obszar, w którym przetwarzane są dane osobowe.

§ 33

1. Ochronę fizyczną pomieszczeń z komputerami oraz urządzeniami sieciowymi Przychodni w Woli Uhruskiej stanowią drzwi zamykane na klucz.

2. Klucze od pomieszczenia mogą pobierać wyłącznie:
   a) Administrator Danych
   b) IOD,
   c) Osoba upoważniona przez AD,

§ 34

1. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania ustawowych zadań Przychodni w Woli Uhruskiej i posiadających ważną licencję użytkowania.

§ 35

1. Dostęp do systemów operacyjnych stacji roboczych powinien być chroniony przez nazwę użytkownika i hasło.
2. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Użytkownikom systemu nie wolno udostępniać swojego identyfikatora i hasła innym osobom.
4. Wejście do BIOSu komputera powinno być chronione hasłem.

§ 36

1. Bezprzerwowe zasilanie stacjom roboczym zapewnia stosowanie zasilaczy awaryjnych UPS.
2. W przypadku stacji roboczych, UPS stosuje się w zależności od potrzeb i możliwości finansowych.

§ 37

1. Zapewnieniu ciągłej dostępności informacji służą procedury postępowania w przypadku wydarzeń losowych (np. awaria stacji roboczej, zalanie pomieszczenia itp.).
2. Procedury, o których mowa w ust.1 powinny obejmować uruchomienie systemu w minimalnej konfiguracji udostępniającej zasoby systemu.
3. W przypadku gdyby doszło do ewakuacji należy zapewnić bezpieczeństwo danym.

§ 38

1. Wszystkie stacje robocze muszą posiadać zainstalowany program antywirusowy, z możliwie często aktualizowaną bazą wykrywanych wirusów, sprawdzający w trybie rzeczywistym wszystkie przychodzące i wychodzące pliki. Zabronione jest blokowanie pracy tego programu.
2. Dla zapewnienia ochrony przed wirusami i innymi niepożądanymi kodami sprawdza się wszystkie zbiory przychodzące z sieci rozległej i Internetu.

§ 39

1. Wszelkie naprawy i konserwacje sprzętu i oprogramowania mogą odbywać się tylko w obecności osób uprawnionych.
2. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy dopiero po uzyskaniu zgody IOD lub Administratora Danych.

ROZDZIAŁ XI
OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

§ 40

Zgodnie z art. 4 pkt 12 Rozporządzenia naruszenie ochrony danych osobowych oznacza:

1. Zniszczenie danych osobowych – sytuacja, w której dane przestają istnieć w formie nadającej się do użytku administratora;
2. Zmianę danych osobowych – uszkodzenie (przypadkowe lub niezgodne z prawem) danych w konsekwencji którego stały się niekompletne, częściowo nieczytelne, nieprawidłowe;
3. Utrata danych osobowych – sytuacja, w których dane mogą wprawdzie nadal istnieć, ale administrator danych utracił nad nimi kontrolę lub dostęp, lub nie jest w ich posiadaniu.

Dodatkowo wyróżniamy trzy typy naruszenia ochrony danych osobowych:

1. **Naruszenie poufności** polegające na ujawnieniu danych osobowych nieuprawnionej osobie;
2. **Naruszenie dostępności** jest trwała utrata lub zniszczenie danych osobowych;
3. **Naruszenie integralności** jest to nieautoryzowana zmiana treści danych osobowych.

§ 41

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

1. 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.,
2. niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3. awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a tym sam fakt pozostawienia serwisantów bez nadzoru,
4. pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5. jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6. naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7. stwierdzenie próby lub modyfikacji danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8. wystąpienie niedopuszczalnej manipulacji danymi osobowymi w systemie,
9. ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,
10. 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,
11. ujawnienie istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
12. podmienienie lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
13. rażące naruszenie dyscypliny 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, prace na danych osobowych w celach prywatnych, itp.).

§ 42

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.

ROZDZIAŁ XII
ZASADY POSTĘPOWANIA W SYTUACJI NARUSZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

§ 43

Niniejsze zasady określają tryb postępowania w przypadku 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.

§ 44

O naruszeniu ochrony danych osobowych mogą świadczyć w szczególności następujące symptomy:

1. brak możliwości uruchomienia przez użytkownika programu pozwalającego na dostęp do danych osobowych,
2. brak możliwości zalogowania się do tego programu,

3. ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika programu (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
4. wygląd programu inny niż normalnie,
5. inny zakres danych niż normalnie dostępny dla użytkownika dużo więcej lub dużo mniej danych,
6. znaczne spowolnienie działania systemu informatycznego,
7. pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
8. ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
9. ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii awaryjnych,
10. włamanie lub próby włamania do szafek, w których przechowywane są w postaci elektronicznej lub papierowej - nośniki danych osobowych,
11. zagubienie lub kradzież nośnika danych osobowych,
12. zagubienie lub kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, itp.),
13. kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe,
14. informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
15. fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej,
16. podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

§ 45

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.

§ 46

1. Każdy pracownik Przychodni w Woli Uhruskiej biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania IOD lub innej osoby wskazanej przez niego.
2. Każda osoba zatrudniona w Przychodni w Woli Uhruskiej która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub IOD.
3. W przypadku niemożliwości zawiadomienia IOD lub osób przez niego upoważnionych, pracownik winien powiadomić Administratora Danych.

§ 47

1. Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia danych osobowych przekazywana jest przez pracownika osobiście, telefonicznie lub pocztą elektroniczną.
2. Informacja, o której mowa w ust. 1 powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia.
3. W przypadku gdy zgłoszenie o podejrzeniu zaistnienia incydentu otrzyma osoba inna niż IOD, jest ona obowiązana poinformować o tym fakcie IOD.
4. Pracownik może zostać poproszony przez IOD o potwierdzenie zauważonego faktu na piśmie.

§ 48

1. Do czasu przybycia IOD lub upoważnionej przez niego osoby, zgłaszający:
   a) niezwłocznie podejmuje czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnia w działaniu również ustalenie przyczyn lub sprawców,
   b) zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,

c) wstrzymuje pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
d) nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,
e) podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
f) podejmuje inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
g) powinien wstępnie udokumentować zaistniałe naruszenie.

2. Dokonywanie zmian w miejscu naruszenia ochrony jest dopuszczalne jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

§ 49

Inspektor Ochrony Danych lub osoba przez niego upoważniona, niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych, powinien:

1. zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Przychodni w Woli Uhruskiej,
2. zapisać wszelkie informacje związane z danym zdarzeniem,
3. wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
4. przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
5. wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
6. dokonać zmiany hasła konta użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
7. zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem
8. usunąć skutki incydentu i przywrócić pierwotny stan systemu informatycznego (to jest sprzed incydentu).

§ 50

Administrator Danych niezwłocznie podejmują działania w celu:

1. wyjaśnienia zdarzenia w szczególności czy miało miejsce naruszenie ochrony danych osobowych,
2. wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów w szczególności, gdy zdarzenie było związane z celowym działaniem pracowników bądź osób trzecich,

§ 51

1. Administrator Danych oraz IOD przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych.
2. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:
   a) przeprowadzenie naprawy sprzętu informatycznego,
   b) rekonfigurację sprzętu informatycznego,
   c) wprowadzenie poprawek do oprogramowania,
   d) rekonfigurację oprogramowania,
   e) odtworzenie danych z kopii awaryjnych,
   f) modyfikację danych w celu odtworzenia ich integralności,
   g) wycofanie z użycia materiału kryptograficznego,
   h) inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej i wspomagających lub zabezpieczających działanie systemu informatycznego.

§ 52

1. W sytuacjach wyjątkowych wszystkie powyżej opisane działania związane z usuwaniem skutków incydentu i wyjaśnianiem jego przyczyn mogą być realizowane przez osoby upoważnione przez IOD.
2. Jeżeli incydent był spowodowany celowym działaniem, IOD jest zobowiązany do pisemnego powiadomienia Administratora Danych o zaistniałym zdarzeniu.

3. Administrator Danych, biorąc pod uwagę charakter zdarzenia, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

§ 53

Zgodę na uruchomienie komputerów i innych urządzeń lub dokonanie zmian w miejscu naruszenia ochrony wyraża IOD lub osoba przez niego upoważniona.

§ 54

1. System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu. W czasie jej trwania użytkowanie systemu informatycznego powinno być ograniczone do niezbędnego minimum.
2. Okres kwarantanny, o którym mowa w ust.1, jest uzależniony charakterem incydentu i specyfiką systemu informatycznego.

§ 55

1. W przypadku naruszenia ochrony danych osobowych, administrator danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 Rozporządzenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin Administrator Danych dołączy wyjaśnienie przyczyn opóźnienia.
2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
3. Zgłoszenie, o którym mowa w ust. 1, musi zawierać co najmniej:
   1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
5. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) Rozporządzenia.
6. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   1) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
   3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których
   4) dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§ 56

1. Administrator Danych prowadzi Rejestr Naruszeń Ochrony Danych Osobowych – Załącznik nr 5 do niniejszej Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

ROZDZIAŁ XIII
POSTANOWIENIA KOŃCOWE

§ 57

1. Administrator Danych zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik – Nr 6 do niniejszej Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

§ 58

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym IOD.
2. Nałożona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z Rozporządzeniem lub Ustawą.

§ 59

W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy Rozporządzenia lub Ustawy.

§ 61

Niniejsza polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym może być zmieniana/modyfikowana oraz aktualizowana.