**REGULAMIN OCHRONY DANYCH OSOBOWYCH**

**W**

**„TERVENT" Andrzej Śliwczyński**
**Centrum Medycyny Nowa Europa**
**90-442 Łódź Al. Kościuszki 106/116**

| …… | ……. | …… |
|---|---|---|
| administrator danych osobowych | podpis w imieniu administratora danych osobowych | data |

## Wstęp

Niniejszy Regulamin stanowi doprecyzowanie najistotniejszych zapisów zawartych w dokumentacji ochrony danych osobowych. Obowiązuje pracowników etatowych oraz współpracowników, posiadających ważne upoważnienia do przetwarzania danych osobowych nadane przez administratora danych.

## Nadawanie upoważnień i uprawnień

**1**.Za nadawanie upoważnień do przetwarzania danych osobowych odpowiada osoba do tego umocowana przez Administratora Danych Osobowych - Administrator Systemu Informatycznego

**2.**Osoba nadająca upoważnienia jest niezwłocznie informowana o zatrudnieniu nowego pracownika łub zleceniobiorcy, jak i o zakończeniu stosunku pracy łub umowy zlecenia z osobą upoważnioną.

**3.**Każda osoba przed nadaniem upoważnienia do przetwarzania danych osobowych musi:

a) zapoznać się z niniejszym regulaminem,

b) odbyć szkolenie z zasad ochrony danych osobowych,

c) podpisać oświadczenie o poufności.

**4.**Upoważnienie nadawane jest do przetwarzania danych osobowych w wersji papierowej i/lub systemie informatycznym.

**5**.W przypadku gdy upoważnienie udzielane jest do zbioru w systemie informatycznym, administrator tego systemu nadaje osobie indywidualny i unikalny identyfikator w systemie.

**6.**W przypadku odebrania upoważnienia do przetwarzania danych osobowych, uprawnienia przydzielone w systemie informatycznym osoby są blokowane.

**7.**Administrator systemu odpowiada za rejestrowanie przydzielonych uprawnień w systemie informatycznym oraz za prowadzenie rejestru osób upoważnionych.

## Polityka haseł

**1**.Hasło dostępu do systemu informatycznego składa się co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych)

**2.**Zmiana hasła dostępowego do systemu informatycznego następuje nie rzadziej niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

**3.**Zmianę hasła wymusza system a użytkownik zobowiązany jest do manualnej zmiany hasła.

**4**.Hasła nie mogą być powszechnie używanymi słowami, w szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.

**5**.Osoba posiadająca dostęp do systemu informatycznego zachowuje hasło w poufności, nawet po jego zmianie na nowe, w szczególności zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

## Użytkowanie systemu informatycznego

**1.**Sprzęt informatyczny służący do przetwarzania danych osobowych składa się w szczególności z komputerów stacjonarnych, elektronicznych nośników danych osobowych, sieciowego sprzętu drukującego, infrastruktury sieci LAN oraz stacji serwerowych.

**2**.Osoba korzystająca z systemu informatycznego.

a) jest zobowiązana do użytku sprzętu w sposób zgodny z jego przeznaczeniem oraz do ochrony sprzętu przed zniszczeniem, utratą lub uszkodzeniem,

b) jest zobowiązana do informowania administratora tego systemu o każdej sytuacji zniszczenia, utraty lub uszkodzenia powierzonego sprzętu,

c) nie może instalować samowolnie żadnego oprogramowania w systemie informatycznym, ani próbować złamać lub uzyskać uprawnienia administracyjne w tym systemie,

d) nie może samowolnie otwierać (demontować) sprzętu, instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego (w tym prywatnych urządzeń, nawet jedynie w celu ładowania baterii tych urządzeń).

## Polityka czystego ekranu

**1.**Osoba korzystająca z systemu informatycznego jest zobowiązana do zachowania polityki czystego ekranu, tj. zapewnienia, by osoby nieupoważnione nie miały wglądu w treści wyświetlane na monitorach ekranowych lub ekranach komputerów przenośnych.

**2**.Osoba korzystająca z systemu informatycznego jest zobowiązana do manualnego uruchamia wygaszacza ekranu chronionego hasłem w każdej sytuacji, gdy pozostawia system informatyczny bez nadzoru (nawet na chwilę).

**3**.Zabronione jest gromadzenie danych osobowych w postaci tzw. zrzutów ekranów z systemu informatycznego, jak i wysyłanie takich informacji poza organizację bez zgody administratora tego systemu.

**4**.Osoby korzystające z systemu informatycznego powinny zwracać szczególną uwagę na:

a) ustawienie monitorów lub ekranów komputerów przenośnych w obszarze przetwarzania względem okien (w przypadku blisko siebie sąsiadujących budynków) oraz drzwi wejściowych, przez które mogą wejść osoby nieupoważnione,

b) uruchamianie komputerów przenośnych poza obszarem przetwarzania w miejscach publicznie dostępnych (np. lotniska, dworce, sale konferencyjne itp.),

c) osoby nieupoważnione pozostające w obszarze przetwarzania danych bez nadzoru osób upoważnionych.

## Polityka czystego biurka i czystego druku

**1.**Osoba przetwarzająca dane osobowe jest zobowiązana do zachowania polityki czystego biurka, tj. zapewnienia by po zakończeniu pracy wszelkie dane osobowe zarówno w wersji papierowej, jak i na elektronicznych nośnikach znajdowały się poza zasięgiem wzroku i dłoni.

**2.**Osoba przetwarzająca dane osobowe jest zobowiązana do stosowania wszelkich zabezpieczeń danych udostępnionych przez administratora danych, tj. jeżeli pomieszczenie jest zaopatrzone w meble zamykane na klucz, to należy zamykać szafy przed zakończeniem pracy, a klucze umieszczać w bezpiecznym miejscu.

**3.**Ostatnia osoba opuszczająca obszar przetwarzania jest zobowiązana do sprawdzenia, czy wszystkie okna są zamknięte (ryzyko zalania pomieszczeń lub włamania) oraz czy wszelkie inne zabezpieczenia są uruchomione (np. system alarmowy należy uzbroić, drzwi należy zamknąć).

**4.**Zabrania się pozostawiania wydruków zawierających dane osobowe w pobliżu urządzeń drukujących bez nadzoru; dokumenty błędnie wydrukowane należy niezwłocznie niszczyć z wykorzystaniem niszczarek lub pojemników do utylizacji dokumentacji poufnej.

**5.**Przewożenie poza obszarem przetwarzania wersji papierowej danych osobowych musi odbywać się w sposób zapewniający ich poufność, tj. dokumenty muszą być zakryte i zabezpieczone przed przypadkową utratą.

## Udostępnianie danych osobowych

**1.**Osoba przetwarzająca dane osobowe może udostępniać dane osobowe drogą telefoniczną jedynie wtedy, gdy ma pewność co do tożsamości swojego rozmówcy (w razie wątpliwości należy weryfikować tożsamość np. poprzez żądanie podania fragmentu informacji znanej tylko osobie właściwej np. PESEL, nr dokumentu, nazwisko lekarza, data ostatniej wizyty itd.).

**2.**Dane osobowe można udostępnić tylko osobie, której dane dotyczą, lub innej osobie za jej zgodą przechowywaną w celach dowodowych przy zachowaniu procedury przewidzianej w punkcie powyższym.

**3.**Udostępniając dane osobowe w miejscach publicznie dostępnych, należy zagwarantować poufność danych. Jeżeli ustne przekazanie danych nie gwarantuje poufności, należy skorzystać z udostępnienia w wersji pisemnej (do wglądu).

**4.**Należy zwracać uwagę na sytuacje mogące stanowić ryzyko ujawnienia danych osobowych lub informacji o stosowanych zabezpieczeniach osobie nieupoważnionej, takie jak:

a) żądanie udostępnienia danych przez osoby podszywające się (kradzież tożsamości),

b) żądanie udostępnienia informacji o stosowanych zabezpieczeniach, w tym w szczególności udostępnienia obecnych, jak i poprzednio stosowanych haseł dostępowych do systemów informatycznych (socjotechnika telefoniczna),

c) wszelkie inne nieuzasadnione i podejrzane żądania udostępnienia informacji, w szczególności drogą telefoniczną

## Korzystanie z dostępu do Internetu

**1**.Osoby przetwarzające dane mają prawo korzystać z dostępu do Internetu jedynie w celu wykonywania obowiązków na zajmowanym stanowisku.

**2.**Przy korzystaniu z Internetu osoby przetwarzające dane mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.

**3.**Osoby przetwarzające dane nie maja prawa korzystania z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym.

**4.**W zakresie dozwolonym przepisami prawa administrator danych zastrzega sobie prawo kontrolowania sposobu korzystania przez osoby przetwarzające dane z Internetu pod kątem wyżej opisanych zasad.

**5.„TERVENT" Andrzej Śliwczyński Centrum Medycyny Nowa Europa, (90-442) Łódź, al. Kościuszki 106/116** może udostępnić internet dla ……..poprzez WiFi wyłącznie na zasadach opisanych i zatwierdzonych przez Administratora Danych Osobowych w regulaminie.

## Korzystanie z poczty elektronicznej

**1.**Poczta elektroniczna jest przeznaczona wyłącznie do wykonywania obowiązków na zajmowanym stanowisku.

**2.**Przy korzystaniu z poczty elektronicznej osoby przetwarzające dane mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.

**3.**Osoby przetwarzające dane nie mają prawa wysyłać wiadomości zawierających informacje określone jako poufne, dotyczące administratora danych, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

**4.**Osoby przetwarzające dane nie powinny otwierać wiadomości przesłanych droga elektroniczną od nieznanych sobie nadawców, gdy tytuł nie sugeruje związku z wypełnianymi przez nie obowiązkami na zajmowanym stanowisku.

**5.**Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesłanych pocztą elektroniczną.

**6.**W przypadku przesyłania plików zawierających dane osobowe, dane wrażliwe do podmiotów zewnętrznych, osoba przetwarzająca dane zobowiązana jest do ich spakowania i opatrzenia hasłem. Hasło należy przesłać odrębnymi środkami komunikacji ( np.SMS).

**7.**Udostępnianie danych musi być odnotowane a osoba przetwarzająca dane musi uzyskać potwierdzenie wystąpienia o udostępnienie danych przez właściwą osobę oraz pokwitowanie odebrania danych w postaci tworzącej stały dowód ( np. wydruk korespondencji elektronicznej).

## Elektroniczne nośniki danych

**1**.Elektroniczne nośniki danych to np. wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.

**2**.Osoby przetwarzające dane nie mogą wynosić poza obszar przetwarzania wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora Danych Osobowych.

**3.**W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik przez spalenie lub rozdrobnienie.

## Instrukcja alarmowa

**1.** Osoba przetwarzająca dane zobowiązana jest do powiadomienia administratora danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, w szczególności gdy:

a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,

b) dokumentacja jest niszczona bez użycia niszczarki,

c) drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, pozostają otwarte,

d) ustawienie monitorów pozwala na wgląd osób nieupoważnionych,

e) ma miejsce nieautoryzowane wynoszenie danych osobowych w wersji papierowej i/lub elektronicznej poza obszar przetwarzania,

f) występują telefoniczne próby wyłudzenia danych osobowych,

g) nastąpiła kradzież komputerów lub elektronicznych nośników danych,

h) pojawia się zagrożenie notyfikowane przez program antywirusowy,

i) hasła do systemów przechowywane są w pobliżu komputera.

**Postępowanie dyscyplinarne**

**1.**Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego Regulaminu mogą zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub zobowiązań umownych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego podejrzenia takiego naruszenia nie podjęła działania określonego w niniejszym Regulaminie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, można wszcząć postępowanie dyscyplinarne.

**2.**Kara dyscyplinarna zastosowana wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z **Rozporządzeniem 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** (ogólne rozporządzenie o ochronie danych). oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez administratora danych o zrekompensowanie poniesionych strat.