Niniejszy dokument reguluje zasady przetwarzania danych osobowych przez administratora (zdefiniowanego poniżej) i stanowi politykę ochrony danych osobowych w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), zwanego dalej „RODO":

I. Definicje

Ilekroć w niniejszej polityce ochrony danych osobowych użyto słowa lub sformułowania:

1. „administrator" oznacza to **NZOZ Care Point Spółka z ograniczoną odpowiedzialnością z siedzibą w Katowicach**, adres siedziby: 40-750 Katowice, ul. Zdzisława Hierowskiego 68/13, wpisany do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Katowice Wschód w Katowicach, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000608855, REGON: 364026871, NIP: 6372197462, wpisany do rejestru podmiotów wykonujących działalność leczniczą pod nr 000000256580, która ustala cele i sposoby przetwarzania danych osobowych,
2. „dane osobowe" oznacza to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (przy czym, możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować),
3. „system informatyczny" oznacza to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych osobowych przez administratora,
4. „użytkownik" oznacza to pracownika lub współpracownika administratora upoważnionego przez administratora do przetwarzania danych osobowych,
5. „zbiór danych" oznacza to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
6. „przetwarzanie" oznacza to operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
7. „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,
8. „polityka ochrony" lub „niniejsza polityka" oznacza to niniejszą politykę ochrony danych osobowych.

II. Postanowienia ogólne

1. Polityka ochrony została sporządzona w celu zagwarantowania przestrzegania u administratora podczas przetwarzania danych osobowych przepisów RODO oraz innych przepisów prawa dotyczących zasad przetwarzania i zabezpieczenia danych osobowych.
2. Polityka ochrony dotyczy wszystkich danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający, niezależnie od formy ich przetwarzania oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
3. Polityka ochrony jest przechowywana w wersji papierowej każdorazowo w miejscu udzielania świadczeń zdrowotnych przez NZOZ Care Point Sp. z o.o. z siedzibą w Katowicach oraz w siedzibie administratora wskazanej w niniejszej polityce.
4. Polityka ochrony jest udostępniana w wersji papierowej każdorazowo w miejscu udzielania świadczeń zdrowotnych przez NZOZ Care Point Sp. z o.o. z siedzibą w Katowicach oraz w siedzibie administratora wskazanej w niniejszej polityce w formie i w sposób ustalony przez administratora do wglądu na każdy wniosek osobom, których dane osobowe są przetwarzane, upoważnionym, podmiotom przetwarzającym, oraz pracownikom i współpracownikom administratora, którym ma zostać nadane przez niego upoważnienie do przetwarzania danych osobowych lub powierzone przetwarzania danych osobowych, a także w żądanej formie i terminie uprawnionym organom, w szczególności organom nadzoru.
5. Dla skutecznej realizacji polityki ochrony administrator zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych osobowych środki techniczne i rozwiązania organizacyjne,
   b) kontrolę i nadzór nad przetwarzaniem danych osobowych,
   c) monitorowanie zastosowanych środków ochrony.

6. Monitorowanie przez administratora zastosowanych środków ochrony obejmuje w szczególności działania podmiotów przetwarzających i użytkowników, naruszanie zasad dostępu do danych osobowych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi i wewnętrznymi systemu informatycznego.
7. Administrator realizując nadrzędny cel, jakim jest poszanowanie prywatności osób, których dane dotyczą, zapewnia, iż dochowuje wszelkiej staranności, aby dane osobowe tych osób były należycie zabezpieczone przed nieuprawnionym użyciem, ingerencją bądź dostępem osób trzecich oraz, iż czynności wykonywane w związku z przetwarzaniem danych osobowych i ich zabezpieczeniem są zgodne z polityką ochrony oraz odpowiednimi przepisami prawa, w tym z RODO.

III. Dane osobowe przetwarzane u administratora

1. Administrator przetwarza dane osobowe wyłącznie w przypadkach, gdy zachodzi co najmniej jedna z niżej wymienionych przesłanek:
   a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
   b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
   c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
   d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
   e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym przez administratora,
   f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
2. W celu wykonania przedmiotu umowy, w tym powierzenia danych w celu przetwarzania podmiotom współpracującym w zakresie realizacji umowy, Administrator może przetwarzać następujące dane osobowe:
   a) imię,
   b) nazwisko,
   c) PESEL,
   d) nazwa firmy,
   e) NIP,
   f) adres zamieszkania lub siedziby,
   g) płeć,
   h) adres e-mail,
   i) numer telefonu,
   j) informacje o stanie zdrowia i procesie leczenia.
3. Dane osobowe przetwarzane przez administratora gromadzone są w szczególności w zbiorach danych.
4. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z dużym prawdopodobieństwem spowodowania wysokiego ryzyka naruszani praw lub wolności osób fizycznych. Jednakże w przypadku planowania takiego działania administrator zobowiązany jest przed rozpoczęciem przetwarzania dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych zgodnie z postanowieniami art. 35 i następne RODO.
5. W przypadku planowania nowych czynności przetwarzania administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
6. Administrator przetwarza wszelkie dane osobowe w prawnie uzasadnionych celach i zakresie, a w szczególności w przypadku:
   a) pacjentów w celach i zakresie związanych z udzielaniem świadczeń zdrowotnych,
   b) pacjentów w celach i zakresie związanych z wykonywaniem umowy zwartej ze szpitalem,
   c) osób, które wyraziły zgodę na przetwarzanie ich danych osobowych przez administratora w celach i zakresie określonych w takiej zgodzie.
7. Administrator przechowuje dane osobowe przez prawnie uzasadnione okresy, a w szczególności w przypadku:

a) pacjentów w celach i zakresie związanych z udzielaniem świadczeń zdrowotnych, a następnie do czasu zaspokojenia lub upływu okresu przedawnienia ewentualnych roszczeń przysługujących administratorowi od tych osób lub tym osobom od administratora,
b) pacjentów w celach i zakresie związanych z wykonywaniem umowy zwartej ze szpitalem, a następnie do czasu zaspokojenia lub upływu okresu przedawnienia ewentualnych roszczeń przysługujących administratorowi od szpitala lub szpitalowi od administratora,
c) osób, które wyraziły zgodę na przetwarzanie ich danych osobowych do chwili skutecznego cofnięcia tej zgody lub do chwili, kiedy ustanie cel przetwarzania ich danych przez administratora.

8. W każdym przypadku, gdy administrator
   a) zatrudnia powyżej 249 osób, bądź
   b) przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą lub
   c) przetwarzanie nie ma charakteru sporadycznego lub
   d) przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa,

   zobowiązany jest on prowadzić rejestr czynności przetwarzania danych osobowych za zasadach i w zakresie wskazanych w przepisach art. 30 RODO.

IV. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Przetwarzania danych osobowych może następować wyłącznie zgodnie z obowiązującymi przepisami prawa, w tym z RODO, oraz zgodnie z polityką ochrony, a także innymi ewentualnie ustalonymi przez administratora wewnętrznymi procedurami i innymi dokumentami związanymi z przetwarzaniem danych osobowych u administratora.
2. Dane osobowe są:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane te dotyczą,
   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
   d) prawidłowe i w razie potrzeby uaktualniane,
   e) przechowywane w formie umożliwiającej identyfikację osoby, której dane te dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane, a po tym okresie są one pseudomizowane bądź usuwane,
   f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;

   a administrator jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie wykazać ich przestrzeganie.
3. Wobec osoby, której dane te dotyczą, wykonywany jest obowiązek informacyjny w zakresie i zgodnie z treścią postanowień art. 13 i 14 RODO.
4. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności:
   a) naruszenie ochrony systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach,
   b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym,
   c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony,
   d) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,
   e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania,
   f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych,
   g) naruszenie praw osób, których dane są przetwarzane.

5. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia administratora.
6. Administrator może upoważnić swoich pracowników lub współpracowników do przetwarzania danych osobowych, jako użytkowników, po uprzednim zapoznaniu ich z polityką ochrony.
7. Każdy użytkownik zobowiązany jest do:
   a) przestrzegania zakresu nadanego upoważnienia przez administratora,
   b) przetwarzania i ochrony danych osobowych zgodnie z przepisami, w tym RODO, oraz niniejszą polityką,
   c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,
   d) zgłaszania naruszenia ochrony danych osobowych oraz niewłaściwym funkcjonowaniem systemu informatycznego.

V. Obszar przetwarzania danych osobowych

1. Dane osobowe są przetwarzane w pomieszczeniach na terenie pomieszczeń administratora adresem wskazanym w pkt I.1 niniejszej polityki oraz w pomieszczeniach szpitali i przychodni z którym administrator zwarł umowę o udzielanie świadczeń zdrowotnych, w szczególności na komputerach stacjonarnych i przenośnych oraz na przenośnych urządzeniach telefonicznych, jak i w papierowej dokumentacji.
2. Administrator dopuszcza możliwość przetwarzania danych osobowych również na komputerach przenośnych i przenośnych urządzeniach telefonicznych poza jego siedzibą w uzasadnionych przypadkach.

VI. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Za bezpieczeństwo danych osobowych w systemie informatycznym i za właściwy nadzór odpowiedzialny jest administrator.
2. Administrator zapewnia zastosowanie odpowiednich środków technicznych i organizacyjnych niezbędnych w jego ocenie dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
3. Zastosowane środki ochrony powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów informatycznych, rodzajów zbiorów danych i kategorii danych osobowych. Środki te obejmują w szczególności:
   a) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do użytkowników; inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie użytkownika,
   b) zamykanie pomieszczeń, w których przetwarzane są dane osobowe, na czas nieobecności użytkowników, w sposób uniemożliwiający dostęp do nich innych osób,
   c) wykorzystanie zamykanych szaf, szafek i biurek w celu do zabezpieczenia dokumentów zawierających dane osobowe i innych nośników danych osobowych,
   d) wykorzystanie niszczarek do dokumentów w celu skutecznego usuwania dokumentów zawierających dane osobowe,
   e) ochronę systemu informatycznego przed złośliwym oprogramowaniem lub działaniami inicjowanymi z zewnątrz przy użyciu odpowiedniego oprogramowania,
   f) ochronę urządzeń wchodzących w skład systemu informatycznego przed nieuprawnionym dostępem, poprzez uwierzytelnianie na poziomie dostępu do systemu operacyjnego za pomocą indywidualny identyfikatorów użytkownika i haseł, obejmujących ciągi znaków literowych lub cyfrowych jednoznacznie identyfikujący użytkownika w przypadku przetwarzania danych osobowych w systemie informatycznym.
4. Oprócz administratora, do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być dopuszczeni wyłącznie użytkownicy. Po upoważnieniu użytkownika do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje mu nadany identyfikator użytkownika; z chwilą nadania takiego identyfikatora użytkownik może uzyskać dostęp do systemu informatycznego w zakresie odpowiednim do danego upoważnienia.
5. Użytkownik zobowiązany jest do ustanowienia wymaganego przez system informatyczny hasła, które użytkownika zobowiązany jest utrzymywać w tajemnicy, również po upływie jego ważności.
6. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innemu użytkownikowi. Identyfikator użytkownika, który utracił upoważnienie administratora do przetwarzania danych osobowych zostaje wyrejestrowany z systemu informatycznego, a hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w

celu zapobieżenia dalszemu dostępowi tej osoby do danych. Zabrania się używania przez użytkownika identyfikatora lub hasła innego użytkownika.

7. Nośniki z danymi osobowymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą. Zabrania się wynoszenia jakichkolwiek nośników z terenu, o którym mowa w pkt V.1 niniejszej polityki; z zastrzeżeniem postanowień pkt V.2. niniejszej polityki.
8. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej; aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy. W przypadku wykrycia wirusa należy uruchomić program antywirusowy i skontrolować system informatyczny oraz usunąć wirusa z systemu informatycznego przy wykorzystaniu programu antywirusowego. Jeżeli operacja usunięcia wirusa się nie powiedzie, należy zakończyć używanie i odłączyć zainfekowane urządzenie od systemu informatycznego oraz powiadomić o zaistniałej sytuacji administratora.

VII. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych administrator:
   a) w pierwszej kolejności dokonuje oceny prawdopodobieństwa, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, a następnie
   b) bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu, chyba iż jest mało prawdopodobne by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. 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.
3. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

VIII. Prawa osób, których dane dotyczą.

1. Administrator zobowiązany jest przestrzegać lub wykonywać wszystkie wynikające z RODO prawa, które przysługują osobom, których dane osobowe są przetwarzane przez administratora.
2. Osobom, których dane osobowe są przetwarzane przez administratora, przysługują w szczególności następujące prawa:
   a) prawo wglądu i dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych,
   b) prawo do żądania sprostowania lub uzupełnienia nieprawidłowych lub niekompletnych danych osobowych,
   c) prawo do żądania usunięcia danych osobowych („prawo do bycia zapomnianym”),
   d) prawo do żądania ograniczenia przetwarzania danych osobowych,
   e) prawo do przenoszenia danych osobowych,
   f) prawo do sprzeciwu wobec przetwarzania danych osobowych;

   w przypadkach, w zakresie i na zasadach określonych w art. 15 - 20 RODO.
3. W zakresie, w jakim dana osoba, której dane dotyczą, udzieliła administratorowi zgody na przetwarzanie jej danych osobowych, osobie tej przysługuje prawo do jej cofnięcia w dowolnym momencie; przy czym, cofnięcie zgody nie ma wpływu na zgodność z prawem przetwarzania danych osobowych, którego administrator dokonywał na podstawie udzielonej zgody przed jej cofnięciem.
4. Ponadto, każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza RODO, a także ma prawo do wystąpić z odpowiednim żądaniem do sądu, jeżeli uzna, że prawa przysługujące jej na mocy RODO zostały naruszone w wyniku przetwarzania jej danych osobowych z naruszeniem RODO, oraz żądać od administratora odszkodowania za poniesioną szkodę; w przypadkach, w zakresie i na zasadach określonych w art. 77 - 84 RODO.

IX. Powierzenie przetwarzania danych osobowych

1. Administrator może powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu wyłącznie w drodze umowy zawartej w formie pisemnej lub elektronicznej, zgodnie z wymogami wskazanymi dla takich umów w postanowieniach art. 28 RODO.

2. Przed powierzeniem przetwarzania danych osobowych administrator bada czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
3. W przypadku przekazywania administratorowi przez jego kontrahentów danych osobowych innych niż dane osobowe dotyczące tych kontrahentów w celu lub w związku z zawarciem lub wykonywaniem przez administratora umów z tymi kontrahentami, administrator przetwarza takie dane osobowe w imieniu tych kontrahentów, jako podmiot przetwarzający; do przetwarzania tego mają odpowiednie zastosowanie postanowienia niniejszej polityki.

X. Przekazywanie danych do państwa trzeciego lub organizacji międzynarodowych oraz zautomatyzowane podejmowanie decyzji

1. Administrator nie zamierza przekazywać danych osobowych do państwa trzeciego, ani organizacji międzynarodowych; poza sytuacjami, w których następuje to na wniosek osoby, której dane dotyczą.
2. Administrator nie zamierza przetwarzać danych osobowych w oparciu o zautomatyzowane podejmowanie decyzji, w tym w oparciu o profilowanie danych osobowych.

XI. Postanowienia końcowe

1. Kontakt z administratorem w zakresie przetwarzanych danych osobowych możliwy jest w szczególności na następujące sposoby:
   a) listownie na adres: NZOZ Care Point Spółka z ograniczoną odpowiedzialnością, 40-750 Katowice, ul. Zdzisława Hierowskiego 68/13,
   b) w formie wiadomości elektronicznej na adres: kontakt@carepoint.pl
2. W sprawach nieuregulowanych w polityce ochrony stosuje się postanowienia przepisów RODO oraz innych przepisów prawa dotyczących zasad przetwarzania i zabezpieczenia danych osobowych; w przypadku rozbieżności między niniejszą polityką a tymi przepisami pierwszeństwo zastosowania mają te przepisy.