POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

REHACOMPLEX

IRENEUSZ BRYTAN F.P.H.U.
REHACOMPLEX

ul. 3 Maja 102D,
32 – 400 Myślenice

WYDANE DNIA …….2024 R.
PODPIS OSOBY AKCEPTUJĄCEJ ……..

Spis treści

1. Wstęp 2
2. Definicje 4
3. Zakres Polityki Bezpieczeństwa Danych Osobowych 7
4. Zasady ogólne przetwarzania danych osobowych – IRENEUSZ BRYTAN F.P.H.U. REHACOMPLEX 8
5. Ochrona przetwarzania danych osobowych 9
6. Prawa osób, których dane dotyczą 9
7. Organizacja systemu bezpieczeństwa danych osobowych 14
8. Zarządzanie danymi osobowymi i ryzykiem oraz autoryzacja nowych urządzeń i oprogramowania 16
9. Zarządzanie systemami i sieciami 16
10. Bezpieczeństwo danych osobowych w związku z HR 17
11. Bezpieczeństwo fizyczne i środowiskowe 19
12. Zarządzanie incydentami 19
13. Zarządzanie zmianami 21
14. Zgodność z wymaganiami prawnymi i innymi 22
15. Powierzenie przetwarzania danych osobowych 22
16. Udostępnianie danych osobowych 23
17. Polityka czystego biurka i czystego pulpitu 23
18. Praca zdalna 24
19. Polityka stosowania przenośnych urządzeń mobilnych i elektronicznych nośników informacji 25
20. Wynoszenie danych osobowych 26
21. Szkolenia 27
22. Postanowienia końcowe 27
Wykaz załączników: 29

1. Wstęp

1.1 Wprowadzenie

Dane osobowe są jednym z najważniejszych zasobów Administratora, zaś zapewnienie im bezpieczeństwa jest traktowane priorytetowo. W procesach przetwarzania danych osobowych, kluczowe jest stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania danymi osobowymi w taki sposób, aby zapewnić im poufność, integralność i dostępność, a także zapewnić rozliczalność działań podejmowanych zgodnie z niniejszą Polityką Bezpieczeństwa Danych Osobowych.

Niniejsza Polityka Bezpieczeństwa Danych Osobowych przedstawia strategiczne zasady, z których wynikać będą konkretne środki techniczne i organizacyjne, niezbędne dla zapewnienia poufności, integralności, rozliczalności, ciągłości i przejrzystości przetwarzanych danych osobowych, a także sposób ich przepływu.

Z Polityki Bezpieczeństwa Danych Osobowych wynika także bezpieczeństwo fizyczne przetwarzanych danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia ochrony przetwarzanych danych osobowych.

Dane osobowe przetwarzane przez Administratora są chronione na każdym szczeblu i etapie prowadzonej działalności. Z tego względu Administrator podejmuje wszelkie niezbędne działania mające na celu zapewnienie optymalnej ochrony przetwarzanym danym osobowym, a także spełnienia wymaganego poziomu bezpieczeństwa systemów związanych z ich przetwarzaniem. Ochrona danych osobowych jest realizowana m.in. poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez samych użytkowników.

Polityka Bezpieczeństwa Danych Osobowych została opracowana w sposób spełniający wymagania określone w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 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) (Dz. Urz. UE.L.2016.119.1).

Realizację zamierzeń określonych w niniejszej Polityce Bezpieczeństwa Danych Osobowych gwarantują:

1. Wdrożone procedury określające sposób postępowania pracowników, a także odpowiedzialność za bezpieczeństwo przetwarzanych danych osobowych.

2. Systematyczne szkolenia pracowników z bezpieczeństwa danych osobowych i podnoszenie ich świadomości w tym zakresie.
3. Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (m.in. hasła, identyfikatory), zapewniających im dostęp do różnych poziomów – stosownie do indywidualnego zakresu upoważnienia.

Kierownictwo oraz pracownicy zobowiązują się do spełnienia wymagań dotyczących bezpieczeństwa danych osobowych przedstawionych w niniejszej polityce, jak również do ich ciągłego doskonalenia.

Polityka Bezpieczeństwa Danych Osobowych uwzględnia wymagania wywodzące się:

a) ze strategii funkcjonowania,
b) przepisów prawa powszechnie obowiązującego,
c) bieżącego i przewidywanego kontekstu działalności, w którym występują zagrożenia dla bezpieczeństwa danych osobowych.

Polityka Bezpieczeństwa Danych Osobowych jest dokumentem, który ze względu na zmieniające się zagrożenia przetwarzania danych osobowych i zmiany prawa, podlega na bieżąco uaktualnianiu w zakresie procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych.
Właścicielem niniejszej Polityki Bezpieczeństwa Danych Osobowych jest **IRENEUSZ BRYTAN F.P.H.U. REHACOMPLEX.**

1.2 Cel Polityki Bezpieczeństwa Danych Osobowych

Celem Polityki Bezpieczeństwa Danych Osobowych jest:
1. Uzyskanie optymalnego i zgodnego z wymogami obowiązujących przepisów prawa sposobu gromadzenia i przetwarzania danych osobowych, w formie dokumentacji papierowej, jak i w systemach informatycznych.
2. Zapewnienie właściwej ochrony gromadzonym i przetwarzanym danym osobowym.
3. Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy

przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

2. Definicje

1) **Administrator** – podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem jest IRENEUSZ BRYTAN F.P.H.U. REHACOMPLEX.
2) **Aktywa, zasoby** – wszystko to, co w zakresie danych osobowych ma wartość dla Organizacji.
3) **Analiza ryzyka** – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.
4) **Bezpieczeństwo danych osobowych** – zachowanie co najmniej poufności, integralności i dostępności (opcjonalnie mogą być również brane pod uwagę inne kryteria, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność).
5) **Dane biometryczne** – dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.
6) **Dane dotyczące zdrowia** – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.
7) **Dane genetyczne** – dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.
8) **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (art. 4 ust.1 RODO).

9) **Dane osobowe szczególne** – 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 (art. 9 ust.1 RODO).
10) **Dokument** – informacja i jej nośnik.
11) **Dostępność** – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.
12) **Działanie niezgodne** – działanie niespełniające określonych wymagań.
13) **Działanie korygujące** – działanie w celu wyeliminowania przyczyny wykrytej niezgodności lub innej niepożądanej sytuacji.
14) **Incydent związany z bezpieczeństwem danych osobowych** – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne prawdopodobieństwo naruszenia prawodawstwa i zagrażają bezpieczeństwu przetwarzanych informacji.
15) **Integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności informacji.
16) **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
17) **Niezgodność** – niespełnienie ustanowionych wymagań.
18) **Ocena ryzyka** – proces porównywania ryzyka oszacowanego z określonymi kryteriami jego znaczenia.
19) **Odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.
20) **Ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w taki sposób, aby w przyszłości można było zaprzestać ich przetwarzania.
21) **Organizacja** – IRENEUSZ BRYTAN F.P.H.U. REHACOMPLEX, ul. 3 Maja 102D, 32 – 400 Myślenice.
22) **Osoba możliwa do zidentyfikowania** – każda osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne

23) **Osoba trzecia** – każda osoba nieupoważniona i nieuprawniona do dostępu do zbiorów danych osobowych będących w posiadaniu organizacji, a także osoba posiadającą upoważnienia wydanego przez organizację, lecz podejmująca czynności w zakresie przekraczającym ramy jej upoważnienia.
24) **Podmiot przetwarzający** – osoba fizyczna lub prawna, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu i na polecenie Administratora.
25) **Poufność** – zapewnienie dostępu do informacji tylko osobom upoważnionym.
26) **Postępowanie z ryzykiem** – proces wyboru i wdrażania środków modyfikujących ryzyko.
27) **Pracownik** – osoba zatrudniona na podstawie umowy o pracę, ale także na umowie zlecenie lub dzieło. Jako pracownicy są traktowani także stażyści i praktykanci, przetwarzający dany na polecenie Administratora.
28) **Profilowanie** – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
29) **Przedsiębiorca** – osoba fizyczna lub prawna prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą.
30) **Przedstawiciel** – osoba fizyczna lub prawna, mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez Administratora lub podmiot przetwarzający do reprezentowania Administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z RODO.
31) **Przetwarzanie danych osobowych** – 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.
32) **Proces** – działanie lub zbiór działań wykorzystujące zasoby i realizowany w celu umożliwienia przekształcenia wejść w wyjścia. Często wyjście z jednego procesu stanowi bezpośrednie wejście do procesu następnego.
33) **Procedura** – ustalony sposób przeprowadzania działania.

34) **Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji; pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
35) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 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) (Dz. Urz. UE.L.2016.119.1).
36) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych osobowych.
37) **UODO** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
38) **URPP - Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta** z dnia 6 listopada 2008 r.
39) **UIOZ - Ustawa o systemie informacji w ochronie zdrowia** z dnia 28 kwietnia 2011 r.
40) **Usuwanie danych** – wykasowanie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (anonimizacja).
41) **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
42) **Zdarzenie związane z bezpieczeństwem danych osobowych** – określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Danych Osobowych, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.
43) **Zgoda** – zgoda osoby, której dane dotyczą oznaczająca dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

3. Zakres Polityki Bezpieczeństwa Danych Osobowych

Wszystkie osoby, które posiadają dostęp do danych osobowych, zobowiązane są do stosowania zasad i regulacji wynikających z Polityki Bezpieczeństwa Danych Osobowych.

Polityka Bezpieczeństwa Danych Osobowych dotyczy wszystkich pracowników we wszystkich lokalizacjach, w których działalności prowadzi Administrator.

4. Zasady ogólne przetwarzania danych osobowych – IRENEUSZ BRYTAN F.P.H.U. REHACOMPLEX

1) Administrator uwzględniając charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności z RODO.

2) Środkami technicznymi i organizacyjnymi są w szczególności:

a) wdrożenie niniejszej Polityki Bezpieczeństwa Danych Osobowych,
b) dopuszczenie do przetwarzania danych osobowych wyłącznie osób upoważnionych,
c) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
d) bieżące zaznajamianie osób upoważnionych z powszechnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych,
e) zapewnienie przetwarzania danych osobowych w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
f) dopuszczenie do przebywania osób trzecich w pomieszczeniach, gdzie przetwarzane są dane osobowe, tylko w obecności osoby upoważnionej oraz w warunkach zapewniających bezpieczeństwo danych.

3) W celu zapewnienia skutecznego funkcjonowania niniejszej Polityki, Administrator zapewnia:

a) szkolenia w zakresie ochrony danych osobowych w celu stałego podnoszenia wiedzy i świadomości pracowników,
b) odpowiednie do zagrożeń i kategorii danych objętych ochroną zasoby, niezbędne dla funkcjonowania, utrzymania i doskonalenia Polityki,
c) kontrolę i nadzór nad przetwarzaniem danych osobowych, w tym nad przetwarzaniem danych osobowych przez podmioty zewnętrzne, którym dane zostały udostępnione lub powierzone,
d) bieżącą analizę zmieniających się zagrożeń wewnętrznych i zewnętrznych, także z uwzględnianiem zmieniającego się prawa.

4) Odpowiedzialność za bezpieczeństwo przetwarzanych danych osobowych ponoszą wszyscy pracownicy, zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik powinien zostać

zapoznany z zasadami bezpieczeństwa danych osobowych oraz z aktualnymi procedurami ochrony przetwarzanych danych osobowych w miejscu swojej pracy, przed jej rozpoczęciem.
5) Administrator jest odpowiedzialny za nadzorowanie przestrzegania zasad bezpieczeństwa danych osobowych oraz podejmowanie stosownych działań w razie stwierdzenia wystąpienia incydentu lub sytuacji mogącej prowadzić do wystąpienia incydentu bezpieczeństwa danych osobowych.

5. Ochrona przetwarzania danych osobowych

1) Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie, wydane przez Administratora lub osoby przez niego upoważnione – wzór upoważnienia stanowi **załącznik nr 1** do niniejszej polityki.
2) Oświadczenie o ochronie danych osobowych określa zasady poufności danych osobowych oraz odpowiedzialność za ich nieprzestrzeganie, a także obowiązek przestrzegania przepisów z zakresu ochrony danych osobowych – wzór oświadczenia stanowi **załącznik nr 2** do niniejszej polityki.
3) Administrator lub osoby przez niego upoważnione uprawnieni są do nadawania pracownikom upoważnień do przetwarzania danych osobowych, w zakresie szerszym niż wynika z upoważnienia podstawowego, w przypadkach wykonywania przez te osoby innych czynności służbowych nieobjętych zakresem upoważnienia podstawowego.
4) Osoby, które zostały upoważnione do przetwarzania danych osobowych są zobowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia, także po ustaniu współpracy.
5) Administrator prowadzi ewidencję wszystkich osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi **załącznik nr 3** do niniejszej polityki.

6. Prawa osób, których dane dotyczą

1. Osoby, których dane są przetwarzane, mają prawo do ich ochrony poprzez:

1) **Prawo dostępu do swoich danych**, oznaczające, iż:

Osoba, której dane dotyczą jest uprawniona do uzyskania od pracowników Administratora potwierdzenia, czy przetwarzane są jej dane osobowe, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

- cele przetwarzania,
- informacje o kategoriach danych osobowych,

- informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych (jeśli dotyczy),
- w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
- informacje o prawie wniesienia skargi do organu nadzorczego,
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Realizując prawo dostępu do danych konieczne jest odnotowanie tego faktu w wykazie określonym w art. 27 ust. 4 **Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.**

2) <u>Prawo do sprostowania swoich danych</u>, polegające na żądaniu od Administratora niezwłocznego sprostowania danych osobowych.

- Osoba, której dane mają być zmienione/sprostowane, pisemnie informuje Administratora o zakresie danych osobowych wymagających sprostowania.
- Po sprostowaniu danych, Administrator niezwłocznie informuje wszystkich odbiorców danych o tym fakcie.

3) <u>Prawo do usunięcia danych osobowych</u>

W przypadku otrzymania żądania niezwłocznego usunięcia konkretnych danych osobowych, administrator bez zbędnej zwłoki usuwa dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,

- osoba, której dane dotyczą wycofała zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
- osoba, której dane dotyczą zgłosiła sprzeciw wobec przetwarzania swoich danych, w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych,
- dane osobowe były przetwarzane niezgodnie z prawem,
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, przewidzianego w prawie Unii Europejskiej lub prawie Rzeczypospolitej Polskiej,
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

Prawo do usunięcia danych osobowych nie przysługuje, gdy przetwarzanie jest niezbędne do:

- korzystania z prawa do wolności wypowiedzi i informacji,
- wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii Europejskiej lub prawa obowiązującego na terytorium Rzeczypospolitej Polskiej lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej Administratorowi,
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,
- celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1 niniejszego punktu procedury, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania,
- do ustalenia, dochodzenia lub obrony roszczeń.

4) <u>Prawo do ograniczenia przetwarzania danych</u>

Każda osoba, której dane dotyczą (a są przetwarzane przez Administratora), ma prawo żądania ograniczenia przetwarzania w następujących przypadkach:

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający pracownikom Administratora sprawdzić prawidłowość tych danych. W wyniku sprawdzenia prawidłowości danych niezbędne jest sporządzenie notatki stwierdzającej stopień prawidłowości danych,
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

- Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń,
- osoba, której dane dotyczą wniosła sprzeciw, z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, opartego na interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Gdy na podstawie powyższych zapisów, przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania:

- wyłącznie za zgodą osoby, której dane dotyczą, lub
- w celu ustalenia, dochodzenia lub obrony roszczeń, lub
- w celu ochrony praw innej osoby fizycznej lub prawnej, lub
- z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

5) Prawo do przenoszenia danych osobowych

Osoba, której dane dotyczą (a są przetwarzane przez Administratora) ma prawo:

- otrzymać w ustrukturyzowanym, powszechnie używanym formacie (zalecany format to pliki Word lub Excel), nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi,
- przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora, jeżeli:
  – przetwarzanie odbywa się na podstawie wyrażonej zgody (zgodnie z zapisami RODO art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a lub na podstawie umowy w myśl art. 6 ust. 1 lit. b RODO),
  – przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą ma prawo żądania, by dane osobowe zostały przesłane przez Administrator bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

6) Prawo do wniesienia sprzeciwu wobec przetwarzania

Osoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw:

- z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, opartego na interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej administratorowi lub wobec przetwarzania opartego na prawnie uzasadnionych interesach administratora lub strony trzeciej, w tym profilowania na podstawie tych przepisów,

Sprzeciw wniesiony na podstawie wyżej wskazanej przesłanki zobowiązuje Administratora do zaprzestania przetwarzania danych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

- jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego – po jego wniesieniu, Administrator zaprzestaje dalszego przetwarzania danych osobowych w tym celu.

7) <u>Prawo do wycofania zgody na przetwarzanie danych</u>

Prawdo do wycofania zgody przysługuje:

- Osobie, której dane osobowe przetwarzane są na podstawie uprzednio wyrażonej zgody, przysługuje prawo do jej wycofania, zgodnie z art. 7 ust. 3 RODO,
- Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
- Wycofanie zgody powinno być równie łatwe i zrozumiałe, jak jej wyrażenie zgody,
- Wycofanie zgody może być wyrażone w formie papierowej i/lub elektronicznej.

2. Administrator udziela odpowiedzi na wyżej wymienione prawa bez zbędnej zwłoki, jednak nie dłużej niż w ciągu 14 dni. W przypadku, kiedy udzielenie odpowiedzi wymaga dłuższego czasu, Administrator informuje o tym wnioskodawcę.

3. Żądanie realizacji wyżej wskazanych praw składa się poprzez pisemną wiadomość, przekazaną w wersji elektronicznej na adres e-mail: info@rehacomplex.eu lub na adres prowadzonej działalności: ul. 3 Maja 102D, 32 – 400 Myślenice.

4. Poinformowanie o wyżej wymienionych prawa następuje poprzez ich wskazanie w klauzulach informacyjnych – dla pacjentów, kontrahentów, pracowników oraz innych odbiorców.

7. Organizacja systemu bezpieczeństwa danych osobowych

7.1 Zasady ogólne

1) Odpowiedzialność za bezpieczeństwo przetwarzanych danych osobowych ponoszą wszyscy pracownicy, zgodnie z powierzonymi zakresami obowiązków, natomiast za zapewnienie zasobów niezbędnych dla funkcjonowania, utrzymania i doskonalenia niniejszej polityki odpowiedzialny jest Administrator.

2) Administrator decyduje o podjęciu współpracy w zakresie zapewnienia bezpieczeństwa danych osobowych z innymi podmiotami zewnętrznymi.

3) Za nadzorowanie przestrzegania zasad bezpieczeństwa danych osobowych przez pracowników oraz podejmowanie stosownych działań w razie stwierdzenia wystąpienia incydentu lub sytuacji mogącej prowadzić do wystąpienia incydentu bezpieczeństwa, odpowiedzialny jest Administrator lub osoba przez niego wyznaczona.

4) Każdy pracownik zapoznaje się z zasadami bezpieczeństwa danych osobowych oraz z aktualnymi procedurami ochrony przetwarzanych danych osobowych w miejscu swojej pracy, przed jej rozpoczęciem.

5) Poniżej przedstawiono ogólne zasady będące podstawą realizacji Polityki Bezpieczeństwa Danych Osobowych:

- Zasada uprawnionego dostępu – każdy pracownik lub inna osoba przetwarzająca dane osobowe zostaje przeszkolona z zasad ochrony danych osobowych, musi spełniać kryteria dopuszczenia do przetwarzania danych osobowych i podpisać oświadczenie o zachowaniu poufności,
- Zasada przywilejów koniecznych – każdy pracownik lub inna osoba przetwarzająca dane osobowe posiada prawa dostępu do danych osobowych, ograniczone wyłącznie do tych zasobów, które są konieczne do wykonywania powierzonych mu zadań,
- Zasada wiedzy koniecznej – każdy pracownik lub inna osoba przetwarzająca dane osobowe posiada wiedzę o systemie przetwarzania danych osobowych – do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań,
- Zasada asekuracji – każdy mechanizm zabezpieczający ubezpieczony jest drugim, innym mechanizmem,
- Zasada świadomości zbiorowej – wszyscy pracownicy lub inne osoby przetwarzające dane osobowe są świadomi konieczności ochrony przetwarzanych danych osobowych oraz aktywnie uczestniczą w procesie zapewniania ich bezpieczeństwa,

- Zasada indywidualnej odpowiedzialności – za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby,
- Zasada obecności koniecznej – prawo przebywania w określonych miejscach, w których są przetwarzane dane osobowe, mają tylko osoby upoważnione,
- Zasada stałej gotowości – system jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających,
- Zasada najsłabszego ogniwa – poziom bezpieczeństwa danych osobowych wyznacza najsłabszy (najmniej zabezpieczony) element,
- Zasada kompletności – zabezpieczenie jest skuteczne tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania danych osobowych,
- Zasada odpowiedniości – używane mechanizmy są adekwatne do sytuacji,
- Zasada akceptowanej równowagi – podejmowane środki zaradcze nie przekraczają poziomu akceptacji,
- Zasada świadomej konwersacji – nie zawsze i wszędzie mówimy co wiemy, ale zawsze i wszędzie wiemy co, gdzie i do kogo mówimy.

7.2 Zasady współpracy z podmiotami zewnętrznymi i osobami trzecimi

1) Wdrożono standard bezpieczeństwa fizycznego w odniesieniu do podmiotów zewnętrznych i osób trzecich.

2) Pomieszczenia, w których dokonywane jest przetwarzanie danych osobowych wyposażono w fizyczne bariery umożliwiające obsługę podmiotu zewnętrznego lub osoby trzeciej. Fizyczne bariery zostały opisane w punkcie „Bezpieczeństwo fizyczne i środowiskowe".

3) W budynkach i pomieszczeniach Administratora wyodrębnione zostały obszary (strefy bezpieczeństwa) niedostępne dla podmiotów zewnętrznych lub osób trzecich.

4) Każdy podmiot zewnętrzny lub osoba trzecia, która znajduje się w strefie bezpieczeństwa, nie może pozostać bez nadzoru pracownika lub innej osoby upoważnionej.

5) Dostęp do budynków i pomieszczeń nadzorowany jest przez pracowników lub inne osoby upoważnione.

6) Celem zmniejszenia ryzyka, związanego z dostępem podmiotów zewnętrznych do danych osobowych przetwarzanych przez Administratora, uzgadnia się w umowie z podmiotem zewnętrznym, taki jak np. dostawcy usług sieciowych, telekomunikacyjnych, wymagań dotyczących bezpieczeństwa danych osobowych.

8. Zarządzanie danymi osobowymi i ryzykiem oraz autoryzacja nowych urządzeń i oprogramowania

1) Zarządzanie przetwarzanymi danymi osobowymi następuje poprzez zapewnienie im wymaganego poziomu bezpieczeństwa, zgodnie z obowiązującymi przepisami prawa w tym zakresie, ze szczególnym uwzględnieniem wymagań zawartych w RODO oraz UODO.

2) Podczas przetwarzania informacji, dane osobowe są identyfikowane, a następnie klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie zapewnienia odpowiedniego i pożądanego poziomu ich ochrony.

3) Niezwykle istotnym elementem jest przeprowadzanie systematycznej i okresowej analizy ryzyka, jak również opracowania planów postępowania z ryzykiem.

4) Wyniki analizy ryzyka stanowią bezpośrednią podstawę podejmowania wszelkich działań i zapewnienia bezpieczeństwa przetwarzanym danym osobowym.

5) Na podstawie informacji wynikających z przeprowadzonej analizy ryzyka, przygotowywane są plany postępowania z ryzykiem dla kategorii danych osobowych o ryzykach większych niż ustalony poziom ryzyka akceptowalnego.

6) Każde nowe lub zmienione urządzenie lub oprogramowanie służące do przetwarzania danych osobowych lub mogące w jakikolwiek sposób wpływać na określony poziom bezpieczeństwa danych osobowych, musi zostać zweryfikowane i zaakceptowane przez uprawnioną i wskazaną do tego osobę, tj. przez Informatyka.

9. Zarządzanie systemami i sieciami

1) W obiektach Administratora przestrzegane są zasady dotyczące utrzymywania i użytkowania istniejących systemów informatycznych i sieci. Celem tego działania jest zapewnienie przede wszystkim poufności, integralności, dostępności i rozliczalności przetwarzanych danych osobowych. Realizacja tego celu następuje w szczególności poprzez:

a) Weryfikację i monitorowanie na bieżąco funkcjonowania systemów,
b) Zakup i instalację wyłącznie oryginalnych oprogramowań od sprawdzonych producentów,
c) Testowanie oprogramowania przed zakupem,
d) Dokonywanie niezbędnych aktualizacji,
e) Zapewnienie bezpieczeństwa systemów informatycznych za pomocą:
    - szyfrowania połączeń,

- stosowania haseł bezpieczeństwa – hasła te składają się z min. 8 znaków, w tym małych, wielkich liter, cyfr lub znaków specjalnych,
- zmiany hasła co min. 90 dni,
- nadawania indywidualnych identyfikatorów,
- zarządzania przez Informatyka panelem administracyjnym strony www.,
- hasłowania plików wytwarzanych w Pakiecie Office oraz PDF za pomocą Adobe Acrobate,
- usuwania metadanych plików, umieszczanych na serwerze strony www.,
- zainstalowania certyfikatu bezpieczeństwa TLS na stronie www.

f) Wdrożenie ochrony przed szkodliwym oprogramowaniem i wirusami,
g) Przestrzeganie zasad związanych z przekazywaniem aktywów,
h) Przestrzeganie zasad postępowania z nośnikami informacji,
i) Kontrolowanie wprowadzanych zmian do infrastruktury sieciowej,
j) Konserwowanie i naprawę sprzętów, w celu wyeliminowania ich niekontrolowanego wyłączenia i utraty danych osobowych,
k) Wykonywanie kopii zapasowych przetwarzanych danych osobowych,
l) Podnoszenie kompetencji pracowników oraz ich świadomości dotyczącej zapewniania bezpieczeństwa danych osobowych,
m) Niezwłoczne identyfikowanie i ocenę podatności technicznych, w tym błędów i luk w systemach informacyjnych.

Aktualnie wykorzystywane systemy, w których przetwarzane są dane osobowe to:

- ✓ Oprogramowanie Windows 10,
- ✓ Program Antywirusowy,
- ✓ Pakiet Microsoft Office
- ✓ Medi – Portal.

10. Bezpieczeństwo danych osobowych w związku z HR

Zasoby ludzkie oraz sposób zarządzania nimi, stanowią istotne czynniki wpływające na sposób działania Organizacji i są uwzględniane podczas okresowej kontroli ryzyka. Ponadto w ramach przetwarzania danych osobowych pracowników realizowane są wszystkie wytyczne wynikające z RODO i niniejszej polityki, polegające na:

Postępowaniu w ramach rekrutacji:

1) Wobec wszystkich kandydatów realizuje się obowiązek informacyjny oraz pobiera zgody na przetwarzanie danych osobowych w ramach bieżącej rekrutacji i fakultatywnie w przyszłych procesach rekrutacyjnych – wzór klauzuli informacyjnej stanowi **załącznik nr 4** a wzór zgód stanowi **załącznik nr 5** do niniejszej polityki.

2) Niezbędne jest zweryfikowanie tożsamości kandydatów, przystępujących do rozmowy kwalifikacyjnej.

3) Dokumenty aplikacyjne osób nieprzyjętych zostają zniszczone, niezwłocznie po zakończonej rekrutacji.

Postępowaniu wobec pracowników:

1) Weryfikuje się tożsamości pracownika oraz prawdziwości podanych danych, poprzez wgląd do dokumentu tożsamości, weryfikacje świadectw pracy, weryfikacje karalności pracownika (jeżeli wymagane prawem).

2) Wobec wszystkich pracowników, a także zleceniobiorców realizuje się obowiązek informacyjny, wynikający z art. 13 ust. 1 i 2 RODO – wzór klauzul informacyjnych dla pracowników oraz pracowników zatrudnionych na podstawie umowy cywilnoprawnej stanowią kolejno **załączniki nr: 6, 7** do niniejszej polityki.

3) Każdy pracownik pisemnie zobowiązuje się do zachowania poufności, wobec danych osobowych pozyskanych w trakcie trwania umowy.

4) Administrator wydaje pracownikowi upoważnienie do przetwarzania danych osobowych – jeżeli w ramach czynności służbowych przetwarza on dane osobowe – w tym celu wykorzystuje się **załącznik nr 1** do niniejszej polityki.

5) Każdy pracownik zostaje przeszkolony z zakresu bezpieczeństwa danych osobowych i funkcjonowania niniejszej polityki.

6) Jeśli pracownikowi przekazywane są aktywa, korzysta się z protokołu przekazania i/lub z karty obiegowej

7) Jeśli pracownikowi przekazywane są klucze do pomieszczeń, odnotowuje się ten fakt w rejestrze kluczy – wzór rejestru kluczy stanowi **załącznik nr 8** do niniejszej polityki.

Postępowaniu po zakończeniu pracy:

1) Każdemu byłemu pracownikowi jest blokowany i usuwany dostęp do wszelkich systemów informatycznych, w tym do służbowej poczty e-mail.

2) Po zakończeniu współpracy, odbiera się od pracownika wszelkie aktywa, dokumenty i klucze, w których posiadaniu był pracownik.
3) W przypadku zwolnienia lub zakończenia współpracy przed upływem umownego terminu, pracownikowi zostaje cofnięte upoważnienie do przetwarzania danych osobowych.

11. Bezpieczeństwo fizyczne i środowiskowe

1) Dla zapewnienia odpowiednio wysokiego poziomu bezpieczeństwa fizycznego i organizacyjnego, przyjęto standardy, wśród których należy wymienić:
a) Standard bezpieczeństwa fizycznego (osiągany m.in. poprzez fizyczną kontrolę wejść do stref bezpieczeństwa, mechaniczne zabezpieczenie budynków i pomieszczeń, wyznaczenie stref o różnym poziomie bezpieczeństwa),
b) Standard bezpieczeństwa sprzętu (osiągany m.in. poprzez zapewnienie bezpieczeństwa okablowania, odpowiednie rozmieszczenie sprzętu),
c) Standard konfiguracji i eksploatacji sieci (osiągany poprzez zapewnienie bezpieczeństwa usług sieciowych, kontroli wirusów i oprogramowania złośliwego, identyfikację sprzętu w sieci).

Aktualnie stosowane zabezpieczenia fizycznego i środowiskowe:

- pomieszczenia zamykane na klucz,
- stosowanie monitoringu wizyjnego,
- wolnostojące gaśnice zabezpieczające przed skutkami pożaru,
- należyte okablowanie, uniemożliwiające podpięcie się do urządzeń i sieci obcego sprzętu, osoby trzeciej,
- stosowanie kontroli dostępu do archiwum.

12. Zarządzanie incydentami

1) Wszelkie nieprzewidziane działania, sytuacje wpływające na poufność, dostępność i integralność danych osobowych, identyfikowane są jako incydent.
Incydenty mogą polegać na:

- naruszeniu hasła dostępu i identyfikatora,
- wykryciu wirusa komputerowego,
- zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,
- nieumyślnym udostępnieniu danych osobowych w Internecie,

- awariach serwerów, komputerów, twardych dysków, oprogramowania, w wyniku których mogło dojść do utraty bądź zniszczenia przetwarzanych danych osobowych,
- podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających informacje np. księgowe, kadrowe, dane osobowe, dane o klientach,
- zdarzeniach losowych zewnętrznych (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
- włamaniu do obiektów lub pomieszczeń,
- ujawnieniu informacji służbowych bądź danych osobowych osobom nieuprawnionym.

Po wykryciu ww. zjawisk lub innych tego typu, Administrator niezwłocznie podejmuje działania mające na celu zarówno zidentyfikowanie jak i ocenę incydentu. Postepowanie polega na:

I. Zgłoszeniu przez pracownika zauważonych nieprawidłowości do Administratora lub osoby wskazanej – zawiadomienie musi zawierać:

- imię i nazwisko osoby zgłaszającej,
- datę zdarzenia,
- krótki opis sytuacji/nieprawidłowości,

II. Ocenie przez Administratora lub osobę wskazaną czy dana sytuacja stanowi incydent naruszenia bezpieczeństwa danych osobowych.

III. Przekazaniu przez Administratora lub osobę wskazaną informacji na temat incydentu Informatykowi – w przypadku incydentów związanych z systemami informatycznymi bądź urządzeniami komputerowymi.

IV. Określeniu skali zjawiska, w tym zakresu utraconych lub udostępnionych danych osobowych.

V. Podejmowaniu stosownych działań przez Informatyka (w przypadku incydentów informatycznych) i/lub przez Administratora (w przypadku incydentów informatycznych oraz innych), mających na celu przywrócenie pożądanego stanu, takich jak:

- zabezpieczenie danych,
- wylogowanie się ze wszystkich systemów,
- zmiany haseł w systemach informatycznych oraz na urządzeniach,
- zablokowanie operacji bankowych,
- odłączenie urządzeń od sieci.

VI. Przeanalizowaniu dowodów, wykryciu sprawcy incydentu,

VII. Sporządzeniu przez Administratora lub osobę wskazaną i/lub Informatyka protokołu opisującego incydent oraz odznaczeniu tego faktu w rejestrze incydentów (**załącznik nr 12 - wzór rejestru incydentów bezpieczeństwa danych osobowych**).
VIII. Zgłoszeniu incydentu do Urzędu Ochrony Danych Osobowych w ciągu 72 godzin od dowiedzenia się o nim, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
IX. Poinformowaniu osób, których dane osobowe zostały naruszone o tym fakcie – jeżeli zachodzą ustawowe przesłanki.

13. Zarządzanie zmianami

Administrator jest świadom częstych zmian przepisów prawnych, rozwoju technologicznego, potrzeby szybkiego dostosowywania się do wymagań otoczenia oraz konieczności ciągłego wzrostu efektywności realizowanych działań, jako elementów w sposób znaczący wpływających na wdrożoną i utrzymywaną Politykę Bezpieczeństwa Danych Osobowych. Z uwagi na to zapewnia narzędzia i metody uwzględniające zmiany, tak aby zachować należyty poziom bezpieczeństwa danych osobowych.

Postępowanie polega na:

1) Ustaleniu celu zmiany,
2) Analizowaniu wprowadzonej zmiany dla sposobu funkcjonowania niniejszej polityki,
3) Określeniu momentów krytycznych w procesie wdrażania zmian,
4) Przeprowadzeniu testów, weryfikujących zastosowane zmiany,
5) Informowaniu pracowników o zaistniałych zmianach oraz ich aktywne włącznie w ten proces,
6) Monitorowaniu wszystkich etapów wdrożenia zmian.

W związku z zaistniałymi zmianami, w ramach ich implementacji, a także w przypadku awarii i katastrof, Administrator zapewnia ciągłość działania, związaną z gromadzeniem i przetwarzaniem danych osobowych. Celem tych działań jest zapobieganie przerwom w działalności Administratora.
Zapewnienie ciągłości działania realizowane jest poprzez:

- wykonywanie kopii zapasowych,
- posiadanie sprzętów zapasowych w przypadku awarii sprzętów,

- możliwość pracy zdalnej w przypadku awarii lokalizacji pomieszczeń administracyjnych.

14. Zgodność z wymaganiami prawnymi i innymi

1) Administrator dba o zapewnienie zgodności zasad przetwarzania danych osobowych z przepisami obowiązującego prawa, przyjętymi uwarunkowaniami umownymi i normatywnymi oraz własnymi wypracowanymi standardami. Działania realizowane przez Administratora mające na celu zapewnienie bezpieczeństwa danych osobowych są zgodne przede wszystkim z:

- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 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),
- Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych,
- Ustawą z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta,
- Rozporządzeniem Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania,
- Ustawą z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.

Celem takiego postępowania jest unikanie naruszania przepisów prawa, zobowiązań i obowiązków wynikających z umów oraz wymogów bezpieczeństwa.

15. Powierzenie przetwarzania danych osobowych

1) Administrator może w drodze umowy powierzyć innemu podmiotowi przetwarzanie lub przechowywanie danych osobowych. Podmiot przetwarzający może przechowywać lub przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie powierzenia przetwarzania danych osobowych, stanowiącej **załącznik nr 9 do niniejszej polityki.**

2) Powierzając przetwarzanie danych osobowych należy korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie to spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

3) Umowa powierzenia przetwarzania określa przede wszystkim zakres i cel przetwarzania, ale także uprawnienia Administratora oraz zakres odpowiedzialności podmiotu przetwarzającego

z tytułu niewykonania lub nienależytego wykonania umowy oraz sposób rozwiązania umowy oraz inne niezbędne informacje, wynikające z art. 28 ust. 3 RODO.
4) Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności Administratora za niezgodne z prawem przetwarzanie powierzonych danych.
5) Administrator prowadzi rejestr zawartych umów powierzenia przetwarzania danych osobowych – wzór rejestru stanowi **załącznik nr 10** do niniejszej polityki.

16. Udostępnianie danych osobowych

1) Udostępnianie danych osobowych instytucjom i podmiotom zewnętrznym może odbywać się tylko za pośrednictwem Administratora lub osoby wskazanej, z wyjątkiem sytuacji, gdy udostępnienie danych odbywa się na podstawie umowy zawartej między Administratorem, a odbiorcą lub podmiotem przetwarzającym.
2) Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie danych, ich zakres i przeznaczenie, a także podstawę prawną który obliguje do udostępnienia danych osobowych.
3) Wniosek o udostępnienie danych osobowych przekazywany jest do Administratora, który podejmuje decyzję o udostępnieniu lub odmowie udostępnienia.
4) Administrator udostępnia dane osobowe tylko osobom lub podmiotom, uprawnionym do ich otrzymania na mocy przepisów prawa.
5) Dokumentacja medyczna jest udostępniana zgodnie z art. 26 oraz 27 ust. 1, 2 i 3 URPP.
6) Elektroniczna dokumentacja medyczna, o której mowa w art. 2 pkt 6 ustawy UIOZ, jest udostępniana na zasadach określonych w przepisach tejże ustawy.
7) Administrator prowadzi wykaz udostepnień dokumentacji medycznej, zawierający informacje zgodne z art. 27 ust. 4 URPP.
8) Administrator prowadzi zestawienie podmiotów, do których nastąpiło udostępnienie danych osobowych. Wzór wykazu stanowi **załącznik nr 11** do niniejszej polityki.

17. Polityka czystego biurka i czystego pulpitu

1) W Organizacji prowadzona jest świadoma polityka związana z czystym biurkiem i czystym pulpitem monitora komputerowego.
Polega ona na:

- zakazie przechowywania na pulpitach haseł i pinów,

- hasłowaniu folderów zawierających informacje księgowe, kadrowe, o klientach, a także dane osobowe,
- nieprzechowywaniu folderów na pulpicie,
- automatycznym wylogowaniu się z urządzenia po 5 minutach bezczynności,
- nieumieszczaniu na pulpicie ikon nieautoryzowanych programów,
- rozmieszczeniu pulpitów tyłem do osób postronnych, przebywających w pomieszczeniach,
- zakazie pozostawiania na biurku rzeczy, które zagrażają bezpieczeństwu, są to między innymi:
  - hasła do systemu operacyjnego na karteczkach, zostawiane na biurku,
  - PIN do karty bankowej,
  - token do transakcji bankowych,
  - nieszyfrowane pamięci USB,
  - klucze do archiwum, szaf, innych pomieszczeń biurowych,
  - umowy, listy kontrahentów.

2) Polityka zobowiązuje Administratora do opracowania wewnętrznego systemu przekazywania dokumentacji, tak by nie naruszał on zasad polityki czystego biurka i pustego pulpitu. Polityka ta zobowiązuje również Administratora do zdecydowanego działania w przypadku ujawnienia danych osobowych, w tym do poinformowania o zaistniałej sytuacji organów ścigania.

18. Praca zdalna

1) Wykonywanie pracy zdalnej dopuszczalne jest zarówno na sprzęcie służbowym, przekazanym przez Administratora bądź na sprzęcie prywatnym pracownika.

Praca na sprzęcie prywatnym odbywa się z uwzględnieniem następujących zasad bezpieczeństwa:

- Konieczność utworzenia odrębnego konta użytkownika do pracy służbowej,
- Ustawienie hasła do powyższego konta użytkownika, składającego się z min. 8 znaków,
- Konieczność korzystania tylko z zabezpieczonych i sprawdzonych sieci,
- Logowanie się do systemów służbowych za pomocą VPN,
- Zakaz wykonywania pracy zdalnej w miejscach publicznych, zatłoczonych,
- Zakaz pozostawiania urządzeń mobilnych bez nadzoru w trakcie pracy, bez uprzedniego wylogowania się,

- Ustawienie wygaszacza ekranu, włączającego się po 5 minutach bezczynności,
- Posiadanie aktualnego programu antywirusowego,
- Konieczność korzystania z poczty służbowej na sprzęcie prywatnym, w ramach wykonywania pracy zdalnej.

2) Istnieje możliwość wydania sprzętu służbowego, na prośbę pracownika oraz po wydaniu przez Administratora lub osobę wskazaną stosownego protokołu zdawczo-odbiorczego.
3) Ponadto podczas pacy zdalnej:

- zdalny dostęp do danych osobowych wymaga uwierzytelnienia loginem i hasłem, wydanym przez Administratora lub osobę wskazaną,
- dane osobowe oraz ich transfer zabezpiecza się kryptograficznie, minimum poprzez zaszyfrowanie pliku oraz udostępnienie klucza dostępu inną drogą,
- nie dopuszcza się pozostawiania loginów oraz haseł w miejscach pracy urządzeń mobilnych, tak aby były dostępne dla osób nieupoważnionych,
- nie dopuszcza się pozostawiania urządzeń mobilnych bez uprzedniego wylogowania z systemu,
- na wypadek zniszczenia urządzeń mobilnych dane należy zapisywać na serwerze firmowym,
- po zakończeniu pracy mobilnej na urządzeniu należy usunąć z niego wszelkie służbowe informacje, w tym dane osobowe, w sposób uniemożliwiający ich odzyskanie
- w przypadku jakichkolwiek awarii bądź incydentów bezpieczeństwa informacji, pracownik zobligowany jest do niezwłocznego powiadomienia Administratora lub osoby wskazanej.

19. Polityka stosowania przenośnych urządzeń mobilnych i elektronicznych nośników informacji

1) Pracownicy mogą korzystać na terenie siedziby z przenośnych urządzeń mobilnych (np. służbowe laptopy, tablety, smartfony, itp.) oraz elektronicznych nośników informacji (np. szyfrowanych pamięci typu pendrive, dyski zewnętrzne), dostarczonych, ewidencjonowanych i monitorowanych przez Administratora w celu wykonywania zadań zlecanych w ramach realizowanej przez niego działalności.
2) Użytkownik korzystający z urządzenia przenośnego, zobowiązany jest co najmniej do:

- transportu urządzenia z zachowaniem szczególnej ostrożności, w sposób minimalizujący ryzyko kradzieży lub zniszczenia,

- korzystania z urządzenia w sposób minimalizujący ryzyko dostępu do danych przez osoby nieupoważnione,
- niezezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,
- kopiowania danych osobowych, przetwarzanych na komputerze przenośnym, do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych,
- utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł,
- wykorzystywania haseł odpowiedniej jakości, zgodnie ze szczegółowymi wytycznymi.

20. Wynoszenie danych osobowych

1) Poza miejsca przetwarzania danych osobowych, które stanowią siedzibę Administratora nie wolno wynosić żadnych dokumentów, a także innych nośników zawierających dane osobowe.
2) Zasada ta nie dotyczy pracowników, których zakres obowiązków wymaga dokonywania czynności służbowych z dokumentacją lub nośnikami poza obszarem przetwarzania danych osobowych, a także czynności związanych z przesyłaniem i transportem korespondencji. Jednakże w takiej sytuacji pracownicy są zobowiązani stosować środki zapewniające ochronę powierzonych danych osobowych podczas ich transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, a w szczególności zabezpieczyć te dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Pracownicy w takiej sytuacji ponoszą pełną odpowiedzialność za powierzoną im dokumentację oraz nośniki, znajdujące się poza miejscem przetwarzania danych osobowych.
3) W przypadku pracy zdalnej pracownicy mogą przetwarzać dane osobowe poza siedzibą Administratora, jednak wyłącznie za jego zgodą i z zachowaniem wszelkich zasad bezpieczeństwa, opisanych w niniejszej polityce w punkcie „Praca zdalna”.
4) Każdy pracownik, który podejrzewa, iż mogło dojść do naruszenia bezpieczeństwa danych osobowych lub próby dokonania takiego naruszenia przez osoby nieupoważnione, jest zobowiązany do niezwłocznego poinformowania o powyższym Administratora, który prowadzi postępowanie kontrolne, pod kątem wyjaśnienia okoliczności ewentualnego naruszenia bezpieczeństwa danych osobowych.

5) Odpowiedzialność za bezpieczeństwo dokumentacji lub nośników, wynoszonych poza obszar przetwarzania danych osobowych, ponosi – z chwilą ich pobrania – pracownik, który te dokumenty lub nośniki wyniósł.

6) Każdy pracownik po zakończeniu pracy zobowiązany jest zamknąć w szafach wszelką dokumentację oraz elektroniczne nośniki informacji, zawierające dane osobowe, a następnie osobiście zabezpieczyć klucze, zgodnie z procedurami obowiązującymi w tym zakresie.

21. Szkolenia

1) Każdy pracownik przed dopuszczeniem do pracy, poddawany jest szkoleniu i zapoznawany z co najmniej:

a) dokumentacją dot. ochrony danych osobowych, w tym z niniejszą polityką,

b) funkcjonującymi zasadami ochrony danych osobowych,

c) przepisami RODO, UODO oraz innych aktów prawnych, których znajomość jest konieczna do właściwego wykonywania czynności służbowych.

2) Za organizowanie cyklicznych szkoleń z ochrony danych osobowych, ze szczególnym uwzględnieniem zasad funkcjonowania niniejszej polityki odpowiada Administrator.

3) W każdym przypadku istotnych zmian w przepisach dotyczących ochrony danych osobowych lub zasad funkcjonowania niniejszej polityki, pracownicy zostają zapoznani ze stosownymi przepisami lub zmianami.

4) Udział w szkoleniu dokumentowany jest podpisaniem listy obecności. Szkolenie może być zakończone testem wiedzy.

22. Postanowienia końcowe

1) Każdy pracownik zobowiązany jest do zapoznania się z Polityką Bezpieczeństwa Danych Osobowych.

2) Za złożenie przez pracowników stosownych oświadczeń oraz uzyskanie niezbędnych uprawnień dostępu (do pomieszczeń, systemów informatycznych, danych) odpowiada bezpośredni przełożony.

3) Bieżący nadzór nad przestrzeganiem zasad przyjętych w Polityce Bezpieczeństwa pełni Administrator.

4) Naruszenie świadome lub przypadkowe niniejszej Polityki Bezpieczeństwa Danych Osobowych może spowodować skutki prawne, zgodnie z Regulaminem Pracy, a w

przypadkach zastrzeżonych przez ustawodawcę – karne, wynikające z odpowiedzialności określonej przez przepisy prawa.

5) Wobec pracownika, który w przypadku naruszenia zabezpieczeń niniejszej polityki lub uzasadnionego domniemania takiego naruszenia nie podjął działania określonego w niniejszym dokumencie, a w szczególności nie powiadomił o incydencie Administratora i/lub Informatyka, zgodnie z określonymi procedurami – można wszcząć postępowanie dyscyplinarne.

6) Ewentualna kara dyscyplinarna orzeczona wobec osoby, która uchybiła obowiązkom wskazanym w pkt 4, nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z obowiązującymi przepisami prawa oraz możliwości wytoczenia wobec niej powództwa cywilnego przez pracodawcę o odszkodowanie z tytułu rekompensaty, w związku z poniesionymi stratami.

Wykaz załączników:

Zał. nr 1 Wzór upoważnienia do przetwarzania danych osobowych

Zał. nr 2 Wzór oświadczenia o zachowaniu poufności i ochronie danych osobowych

Zał. nr 3 Wzór ewidencji osób upoważnionych do przetwarzania danych

Zał. nr 4 Klauzula informacyjna – rekrutacja pracownika

Zał. nr 5 Wzór zgody na przetwarzanie danych osobowych w ramach rekrutacji

Zał. nr 6 Klauzula informacyjna - pracownik zatrudniony na podstawie umowy o pracę

Zał. nr 7 Klauzula informacyjna - zleceniobiorca

Zał. nr 8 Wzór rejestru kluczy dostępu do pomieszczeń

Zał. nr 9 Wzór umowy powierzenia przetwarzania danych osobowych

Zał. nr 10 Wzór rejestru umów powierzenia przetwarzania danych osobowych

Zał. nr 11 Wzór rejestru udostępnień danych osobowych

Zał. nr 12 Wzór rejestru incydentów bezpieczeństwa danych osobowych