Polityka ochrony i przetwarzania danych osobowych

Natallia Romanowska prowadząca działalność gospodarczą pod firmą Natallia Romanowska z siedzibą przy ul. Dziesięciny nr 89H lok. 2, 15806 Białystok, NIP: 5140268596, REGON: 022440489

§1
Postanowienia ogólne

1. **Polityka** reguluje prawa i obowiązki **Administratora** związane z przetwarzaniem przez niego **Danych osobowych** zgodnie z aktualnie obowiązującymi przepisami**.**
2. **Polityka** jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu danych osobowych, regulującym zasady przetwarzania, przechowywania i zabezpieczenia **Danych osobowych** przez **Administratora.**

§2
Definicje

Jeżeli w treści **Polityki Przetwarzania Danych Osobowych** nie postanowiono inaczej, niżej wskazane wyrażenia, użyte w jej treści mają następujące znaczenie:

1. **RODO** - Rozporządzenia 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,
2. **Polityka –** Polityka Ochrony i Przetwarzania Danych sporządzona w celu realizacji art. 24 ust 2 Rozporządzenia 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,
3. **Administrator** – Natallia Romanowska prowadząca działalność gospodarczą pod firmą Natallia Romanowska z siedzibą przy ul. Dziesięciny nr 89H lok. 2, 15806 Białystok, NIP: 5140268596, REGON: 022440489, Administrator Przetwarzania Danych Osobowych w rozumieniu **Ustawy.**
4. **Dane osobowe –** dane osobowe w rozumieniu **RODO.**
5. **Ewidencja –** Ewidencja osób upoważnionych do przetwarzania Danych osobowych.

§3
Zakres obowiązywania Polityki

1. **Politykę** stosuje się do przetwarzania **Danych osobowych** niezależnie od sposobu przetwarzania , w tym do przetwarzania **Danych osobowych** w sposób tradycyjny lub przetwarzania w systemach informatycznych.
2. **Polityka** obowiązuje wszystkie osoby, które przetwarzają lub mogą przetwarzać **Dane osobowe** znajdujące się w zbiorach **Administratora.**

§4
Obowiązki Administratora

1. **Administrator** zobowiązuje się dopełnić należytej staranności, tak aby **Dane osobowe** były przetwarzane w sposób zgodny z prawem, w szczególności **RODO**, przy zapewnieniu należytego bezpieczeństwa ich przechowywania, w tym ochrony przed bezprawnym dostępem osób nieuprawnionych.
2. **Administrator** jest odpowiedzialny. za należyte wykonywanie obowiązków wskazanych w pkt. 1.
3. **Administrator**, wykonując obowiązki wskazane w ust. 1, w szczególności:
    1) wydaje osobom trzecim uprawnienia do przetwarzania **Danych osobowych**,
    2) wyznacza cele i sposób realizacji ochrony przechowywania i przetwarzania **Danych osobowych.**

§5

Szczegółowe obowiązki Administratora

Do zakresu obowiązków **Administratora** należy w szczególności:

1) zapewnianie przetwarzania **Danych osobowych** zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą,
2) zbieranie **Danych osobowych** wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie **Danych osobowych** w sposób niezgodny z tymi celami,
3) zbieranie i przetwarzanie **Danych osobowych** wyłącznie w zakresie niezbędnym do celów, dla których są one przetwarzane,
4) zapewnienie aby **Dane osobowe** były prawidłowe i w razie potrzeby uaktualniane, prostowane,
5) zapewnienie aby **Dane osobowe** były przechowywane nie dłużej niż jest to niezbędne dla celów, w których dane te są przetwarzane,
6) kontrola zgodności przetwarzania **Danych osobowych** z przepisami o ochronie danych osobowych,
7) opracowanie i aktualizowanie dokumentacji opisującej sposób przetwarzania **Danych osobowych** i środki zapewniające ochronę przetwarzanych danych osobowych, w szczególności poprzez stworzenie stosownych polityk i procedur,
8) zapewnianie zapoznania osób upoważnionych do przetwarzania **Danych osobowych** z przepisami o ochronie danych osobowych;
9) prowadzenie rejestru czynności przetwarzania danych osobowych zgodnie z art. 30 **RODO**.

§ 6

Nadanie uprawnień w zakresie ochrony danych osobowych pracownikowi

Administrator jest uprawniony:

1) kontrolować właściwe zabezpieczenie systemów informatycznych oraz pomieszczeń, w których przetwarzane są **Dane osobowe**;
2) wydawać polecenia w zakresie dot. bezpieczeństwa **Danych osobowych**;
3) żądać wyjaśnień od wszystkich pracowników oraz osób świadczących na rzecz **Administratora** usługi w sytuacjach naruszenia bezpieczeństwa **Danych osobowych**.

§ 7

Zasady udostępniania Danych osobowych

1. Warunkiem przetwarzania **Danych osobowych** jest uzyskanie upoważnienia do przetwarzania **Danych osobowych** wydanego przez **Administratora.** Podstawową formą udzielenia upoważnienia jest **Ewidencja**.
2. Osoba może otrzymać zgodę **Administratora** po spełnieniu następujących wymogów:
    1) Potrzeba przetwarzania **Danych osobowych** jest uzasadniona i jest zgodna z przepisami **RODO** oraz innych obowiązujących przepisów.
    2) **Administrator** lub osoba przez niego upoważniona pouczy wnioskującego o podstawowych zasadach przetwarzania **Danych osobowych,** oraz o treści dokumentów wewnętrznych stworzonych przez **Administratora**, a mających na celu ochronę **Danych osobowych**.

§8

Ewidencja osób uprawnionych do przetwarzania Danych osobowych

1. **Administrator** prowadzi **Ewidencję**, w której są umieszczane kategorie osób upoważnionych do przetwarzania **Danych osobowych**, w **Ewidencji** znajdują się następujące informacje:
    1) Kategoria osób, których **Dane osobowe** dotyczą,
    2) Kategoria osób uprawnionych do przetwarzania **Danych osobowych** poszczególnych kategorii odnoszących się do rejestru czynności przetwarzania,
    3) Okres nadania uprawnień,
    4) Zakres uprawnień
2. **Administrator** niezwłocznie wprowadza zmiany w **Ewidencji** i odnotowuje wprowadzone w jej treści zmiany w przypadku wystąpienia nowej kategorii osób, których **Dane osobowe** są przez niego przetwarzane lub zmian w zakresie wskazanym w ust 1 pkt 2-4

§9

Zbiory danych osobowych i miejsce ich przetwarzania

1. **Dane osobowe** gromadzone są w zbiorach, których wykaz stanowi rejestr czynności przetwarzania,
2. Zbiory **Danych osobowych** gromadzone są i przetwarzane przy użyciu systemów informatycznych. **Administrator** dopuszcza przetwarzanie danych osobowych w formie tradycyjnej (papierowej), w szczególności w celach archiwizacyjnych.
3. Wykaz programów służących do przetwarzania **Danych osobowych** stanowi załącznik nr 1
4. **Dane osobowe** gromadzone i przetwarzane są w wyłącznie w miejscu prowadzenia działalności przez **Administratora**, tj przy ul. Sybiraków nr 8 lok. U1A, 15204 Białystok
5. Zabrania się przetwarzania **Danych osobowych** poza miejscem wskazanym w pkt. 4.
6. Dostęp do pomieszczeń, gdzie przetwarzane są dane zabezpieczony jest zamykanymi na klucz drzwiami wejściowymi, do których klucze posiada wyłącznie **Administrator**. Wejście główne do budynku, w którym znajdują się pomieszczenia, gdzie przetwarzane

są **Dane osobowe** zabezpieczone jest zamykanymi na klucz drzwiami, do których klucze posiada wyłącznie **Administrator** oraz domofonem .

7. Dostęp do pomieszczeń wskazanych w ust 4 podlega kontroli. Ostatnia osoba wychodząca z pomieszczeń danego dnia ma obowiązek zamknięcia drzwi na klucz i aktywowania systemu alarmowego.

8. Pracowników obowiązuje całkowity zakaz wykonywania jakichkolwiek kopii dokumentacji lub plików zawierających **Dane osobowe** oraz wynoszenia poza pomieszczenia wskazane w ust 4 nośników zawierających **Dane osobowe.**

§10

Zabezpieczenie danych osobowych przechowywanych w formie papierowej

Wszystkie dokumenty mogące zawierać **Dane osobowe** w formie tradycyjnej (papierowej) znajdują się w zabezpieczonej kluczem szafie, do której klucze posiada wyłącznie **Administrator**.

§11

Zabezpieczenia Danych Osobowych przechowywanych w systemie elektronicznym
Postanowienia Ogólne

1. Przetwarzanie **Danych osobowych** w systemie elektronicznym odbywa się wyłącznie na komputerze osobistym **Administratora**.

2. **Dane osobowe** zabezpiecza się przy użyciu środków chroniących dane przed nieuprawnionym pozyskaniem i przetwarzaniem.

3. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające **Dane osobowe**, przeznaczone do:

1) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

4. Kopie zapasowe zbiorów **Danych Osobowych**:

1) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

2) usuwa się niezwłocznie po ustaniu ich użyteczności.

§12

Zabezpieczenia Danych Osobowych w systemie elektronicznym
Postanowienia szczegółowe

1. W systemie informatycznym służącym do przetwarzania **Danych Osobowych** stosuje się mechanizmy kontroli dostępu do tych danych.

2. **Administrator** zapewnia aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

3. System informatyczny służący do przetwarzania **Danych Osobowych** zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

4. Dostęp do systemu informatycznego służącego do przetwarzania **Danych Osobowych** zabezpieczony jest poprzez konieczność uwierzytelniania użytkowników przy uruchomieniu komputera za pomocą indywidualnego identyfikatora i hasła.

5. **Administrator** dokonuje cyklicznej zmiany haseł uwierzytelniających dostęp na następujących zasadach:

1) zmiana następuje nie rzadziej niż co 30 dni,
2) hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne,
3) hasło nie może składać się z żadnych danych odnoszących się do imienia, nazwiska, adresu zamieszkania użytkownika, jego daty urodzenia, danych najbliższych mu osób, lub ich fragmentów,
4) hasło nie może być jednakowe z identyfikatorem użytkownika,
5) zabronione jest korzystanie z uprzednio używanego przez użytkownika hasła.

6. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed nieuprawnionym wykonywaniem kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

7. Uprawnienia do wykonywania kopii zapasowych dokumentacji zawierającej **Dane Osobowe** ma wyłącznie **Administrator.**

8. Kopie zapasowe dokumentacji zawierającej **Dane Osobowe** wykonywane są nie rzadziej niż raz w miesiącu.

9. Wszystkie komputery służące od przetwarzania **Danych Osobowych** zabezpieczone są przy pomocy stale aktualizowanego oprogramowania antywirusowego sprawdzającego także korespondencję e-mail.

10. Wszystkie komputery służące od przetwarzania **Danych Osobowych** mają aktywowane wygaszacze ekranu uruchamiające się automatycznie w przypadku bezczynności użytkownika.

11. Monitory komputerów są ustawione w taki sposób aby uniemożliwić dostęp do danych osobowych osobom nieuprawnionym. Niezależnie od powyższego, każdy użytkownik ma obowiązek wylogowania się z programu z chwilą zakończenia pracy,.

§13
Zasady przetwarzania Danych Osobowych

1. **Dane osobowe** mogą być pozyskiwane bezpośrednio od osób, których te dane dotyczą, poprzez ich przekazanie osobiste, drogą telefoniczną lub w formie poczty elektronicznej a także przez podanie ich poprzez komunikatory mediów społecznościowych.

2. **Dane osobowe** niekompletne, nieaktualne, nieprawdziwe lub zebrane z naruszeniem **Ustawy** albo zbędne do realizacji celu, dla którego zostały zebrane, uzupełnienia, uaktualnia się, prostuje lub usuwa.
3. **Dane osobowe** przetwarzane są wyłącznie przez upoważnione przez **Administratora** osoby w sposób zapewniający bezpieczeństwo przetwarzanych danych.
4. **Dane osobowe** przetwarzane są jedynie w celu, w jakim zostały zgromadzone lub w celu dopuszczalnym przez bezwzględne przepisy prawa i jedynie w zakresie niezbędnym dla ich realizacji.

§ 14

Udostępnienia Danych osobowych osobom trzecim

1. **Administrator** udostępnia **Dane osobowe** wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. **Dane osobowe** mogą być udostępniane:
    1) na podstawie wniosku podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów prawa;
    2) na podstawie umowy z zawartej z podmiotem trzecim, w ramach której istnieje konieczność udostępnienia danych;
    3) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o udostępnienie **Danych osobowych** powinien zawierać informacje umożliwiające wyszukanie żądanych **Danych osobowych** w zbiorze oraz wskazywać ich zakres i przeznaczenie.
4. Udostępniając **Dane Osobowe**, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. Odmowa udostępnienia **Danych osobowych** następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli **Dane Osobowe** nie mają związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

§ 15

Usuwanie Danych Osobowych

1. **Dane Osobowe** są przechowywane w sposób umożliwiający identyfikację osób, których dotyczą nie dłużej, niż wymaga tego cel, w którym są przetwarzane lub bezwzględnie obowiązujące przepisy prawa.
2. Decyzję o usunięciu danych lub o zniszczeniu nośników danych podejmuje Administrator, po upływie okresu wskazanego w art. 29 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2009 Nr 52, poz. 417 t.j. Dz.U. z 2017 r. poz. 1318).
3. Nośniki zawierające **Dane Osobowe** są niszczone pod nadzorem **Administratora** w obszarze przeznaczonym do przetwarzania danych. Z czynności tej sporządza się protokół.
4. Na podstawie umowy o powierzenie danych osobowych, **Dane Osobowe** oraz nośniki **Danych Osobowych** mogą być usuwane i niszczone przez podmiot, któremu powierzono **Dane Osobowe**, w sposób uniemożliwiający zapoznanie się z danymi przez osoby nieupoważnione.

§16

Gwarancja praw osoby, której dane dotyczą

1. Na wniosek osoby, której dane dotyczą, **Administrator** zobowiązany jest w terminie 30 dni poinformować ją o przysługujących jej prawach oraz udzielić informacji o których mowa w art. 15 **RODO** poprzez wskazanie
    a) celów przetwarzania,
    b) kategorii przetwarzanych danych,
    c) informacji o podmiotach, którym dane mogą być przekazane.,
    d) okresu planowanego przechowywania danych,
    e) informacji o prawie do żądania sprostowania lub ograniczenia przetwarzanych danych osobowych,
    f) informacji o prawie wniesienia sprzeciwu w przypadkach określonych prawem,
    g) informacji o prawie wniesienia skargi do organu nadzorczego.
2. Jeśli wnioskodawca nie wskaże inaczej, kopia danych osobowych podlegających przetwarzaniu zostanie przekazana wnioskodawcy drogą poczty elektronicznej.
3. Osoba, której dane dotyczą, ma prawo do sprostowania **Danych Osobowych**, w szczególności jeśli dane te są niekompletne lub nieaktualne. **Administrator** dokonuje sprostowania niezwłocznie po otrzymaniu wniosku.
4. Osoba, której dane dotyczą, w przypadkach wskazanych w art. 18 **RODO**, jest uprawniona do żądania od **Administratora** ograniczenia przetwarzania jej danych. W przypadku otrzymania takiego żądania **Administrator** niezwłocznie dokonuje ograniczenia przetwarzania **Danych osobowych** w zakresie wskazanym w żądaniu.
5. W przypadkach określonych w pkt 3-4, **Administrator** niezwłocznie informuje o sprostowaniu lub ograniczeniu przetwarzania **Danych osobowych** każdego odbiorcę, któremu ujawniono **Dane osobowe**, chyba że okaże się to niemożliwe lub wymagać będzie niewspółmiernie dużego wysiłku. **Administrator** informuje osobę, której dane dotyczą o tych odbiorcach, jeżeli osoba, której dane dotyczą tego zażąda.

§17

Postanowienia Końcowe

1. **Polityka** wchodzi w życie z dniem 25.05.2018 r.
2. Zmiana **Polityki** może zostać dokonana w każdym czasie, z 14 dniowym wyprzedzeniem.