Wprowadzona Zarządzeniem Nr 2/2018 z dnia 18.05.2018 r.
Dyrektora Gminnego Ośrodka Zdrowia Trąbki Wielkie

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W GMINNYM OŚRODKU ZDROWIA TRĄBKI WIELKIE SAMODZIELNY PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ

§ 1.

Niniejsza polityka bezpieczeństwa przetwarzania danych osobowych została wdrożona w podmiocie leczniczym w Gminnym Ośrodku Zdrowia Trąbki Wielkie Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej będącej Administratorem Danych Osobowych i zawiera szczegółowe zasady nadzoru i ochrony nad przetwarzaniem danych osobowych.

§ 2.

Każdorazowe naruszenie zasad Polityki może być uznane za poważne naruszenie podstawowych obowiązków pracowniczych lub wynikających z umów cywilnych o współpracy i może skutkować konsekwencjami, zgodnie z Kodeksem Pracy lub odpowiednimi przepisami regulującymi zasady współpracy, jak również z odpowiedzialnością przewidzianą w ustawie o Ochronie Danych Osobowych.

§ 3.

Celem niniejszej Polityki jest ochrona osób fizycznych w związku z przetwarzaniem danych osobowych. Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych.

§ 4.

Przedmiotem Polityki jest określenie, opisanie i zawarcie w tym i załączonych dokumentach, zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych osobowych objętych ochroną, a w szczególności zabezpieczeń danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 5.

Opracowanie niniejszej polityki wynika z:

1) 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 danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej zwane również *„RODO”*;

2) Ustawy z dnia 10 maja o ochronie danych osobowych (DZ. U. poz. 1000);

3) Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, a w szczególności przepisy rozdziału 7;

4) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące

do przetwarzania danych osobowych;

5) Rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

§ 6.

Użyte w niniejszej Polityce definicje określenia oznaczają:

1) **Dane Osobowe** – oznaczają informacje o zidentyfikowanej osobie fizycznej. 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.

2) **Przetwarzanie** – oznacza operację lub zestaw operacyjny wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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.

3) **Ograniczenie przetwarzania** – oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

4) **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub graficznie.

5) **Administrator** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby przetwarzania są określone w prawie Unii lub prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

6) **Podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

7) **Odbiorca** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogę otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych

przez te organy publiczne musi być zgodne z przepisami o ochronie danych mających zastosowanie do celów przetwarzania.

8) **Zgoda** – osoby, której dane dotyczą oznacza 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.

9) **Naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawniania lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

10) **Przedstawiciel** – oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia.

§ 7.

Dokument ten jest przechowywany i aktualizowany w wersji papierowej oraz elektronicznej ze względu na zachowanie czytelności i różnorodności obszarów, w których przetwarzane są dane osobowe. Niniejszy dokument jest regularnie przeglądany i aktualizowany przez Administratora Danych lub Inspektora Ochrony Danych Osobowych (jeżeli został powołany).

Zmiany w dokumencie Polityki oraz załącznikach wprowadzone są w chwili pojawienia się ważnych okoliczności lub nowego przepisu, istotnego dla spójności i aktualności Polityki, bądź aktualizacji dotychczasowych przepisów dotyczących ochrony lub przetwarzania danych osobowych. Zmiany zatwierdzane są przez Administratora Danych.

Informacje o zmianach podawane są do wiadomości osób uczestniczących w przetwarzaniu danych osobowych poprzez publikację na tablicy ogłoszeniowej i informacji wysłanej drogą elektroniczną, dla osób posiadających pocztę email.

W przypadku zatwierdzenia nowej wersji Polityki jest ona drukowana, a wydruk dołączany jest do prowadzonej dokumentacji ochrony danych osobowych. Załączniki są przechowywane w formie elektronicznej i papierowej.

§ 8

I. Zadania Administratora danych.

1) Administrator danych zobowiązany jest zastosować środki techniczne i organizacyjne

zapewniające ochronę przetwarzanych danych osobowych, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

2) Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”);
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 („integralność i poufność”).

3) Administrator danych wyznacza IOD w przypadkach, w których RODO wprowadza taki obowiązek, lub w sytuacji, gdy sam uzna to za konieczne;

4) Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych. Osoby te są zobowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczania;

5) Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane;

6) Administrator Danych ze względu na ciążące na nim obowiązki wynikające z Rozporządzenia 2016/679 art. 35 i 36 o ochronie danych osobowych zobowiązany jest do zastosowania środków technicznych i organizacyjnych, które mają zapewnić ochronę danych osobowych, w świetle adekwatnych zagrożeń, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianę, utratą, uszkodzeniem lub zniszczeniem.

II. Zadania IOD – jeżeli został powołany:

1) Nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających należytą ochronę przetwarzanych danych osobowych;

2) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych (wzory/załączniki);

3) Przeprowadzanie szkoleń dla osób upoważnionych do przetwarzania danych osobowych w zakresie zabezpieczenia Systemu informatycznego;

4) Zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami prawa dotyczącymi ochrony danych osobowych oraz dokumentacją opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych, wdrożoną przez Administratora;

5) Odebranie od osób upoważnionych do przetwarzania danych osobowych oświadczeń o zapoznaniu z przepisami dot. ochrony danych osobowych oraz zobowiązań do zachowania tajemnicy (wzór/załączniki);

6) Prowadzenie pełnej dokumentacji dotyczącej ochrony danych osobowych oraz dbanie o jej aktualność;

7) Weryfikowanie oprogramowania eksploatowanego przy przetwarzaniu danych pod kątem zgodności z przepisami o ochronie danych osobowych;

8) Podejmowanie odpowiednich działań w przypadku naruszeń ochrony danych;

9) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia bezpieczeństwa danych osobowych;

10) Umożliwienie, osobom których dane dotyczą, wglądu do swoich danych oraz pomoc w zakresie zmiany lub usunięcia ich danych osobowych. Na żądanie osoby zainteresowanej może zostać sporządzony wydruk z zapisem jej danych. Na wydruku tym mogą znaleźć się wyłącznie dane osoby zainteresowanej;

11) Udostępnianie przetwarzanych danych osobowych jedynie osobom lub instytucjom uprawnionym do ich pozyskania i przetwarzania;

12) Za właściwe zabezpieczenie zbiorów danych osobowych osób zatrudnionych i współpracujących z Spółką, zgodnie z postanowieniami niniejszej Polityki, odpowiedzialne są osoby gromadzące i przetwarzające te dane w związku z wykonywaniem obowiązków służbowych i innych prac na rzecz Administratora danych;

13) IOD odpowiedzialny jest za przechowywanie upoważnień, wydanych pracownikom i osobom współpracującym na podstawie umów cywilno-prawnych lub za

pośrednictwem firm trzecich. Upoważnienia i oświadczenia pracowników są przechowywane w dokumentach związanych z ochroną danych osobowych;

14) Wszystkie osoby mające dostęp do zbiorów danych osobowych zobowiązane są odbyć szkolenie z zakresu ochrony danych osobowych oraz przestrzegać wymogów ochrony danych osobowych określonych odpowiednimi przepisami prawa, jak również niniejszą Instrukcją oraz Polityką określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Udział w szkoleniach potwierdzany jest na liście obecności (wzory/załączniki).

Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego. Administrator oraz podmiot przetwarzający wspierają Inspektora Ochrony Danych w wypełnianiu przez niego zadań, o których mowa w Rozporządzeniu 2016/679 art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

III. Zadania pracowników i współpracowników.

1) Wszyscy pracownicy i współpracownicy (dalej łącznie zwani *„pracownikami”*) mają obowiązek przestrzegać postanowień zawartych w niniejszej Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym;

2) Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy pracownik zobowiązany jest do zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w tym z niniejszą Polityką. Zapoznanie z niniejszą polityką zostaje potwierdzone podpisem na oświadczeniu. Oświadczenie podlega włączeniu do dokumentów związanych z ochroną danych osobowych;

3) Pracownicy są zobowiązani zadbać o bezpieczeństwo powierzonych im danych osobowych, archiwizowania ich i przechowywania zgodnie z obowiązującą w placówce Polityką bezpieczeństwa, w tym między innymi:

a) chronić dane przed dostępem osób nieupoważnionych,
b) chronić dane przed przypadkowym zniszczeniem, utratą lub modyfikacją,
c) chronić komputery nośnik pamięci, magnetyczne, optyczne zawierające dane osobowe oraz wszelkiego rodzaju druki i wydruki, przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
d) utrzymywać porządek w miejscu przetwarzania danych osobowych, chronić hasło do komputera i programów.

4) Zabrania się pracownikom:

a) ujawniać dane, w tym dane osobowe zawarte w obsługiwanych systemach,
b) kopiować bazy danych lub ich części bez wyraźnego upoważnienia,
c) przetwarzać danych osobowych w sposób inny, niż wynika to z obowiązujących

przepisów prawa.

5) Pracownicy zobowiązani są do udzielania pomocy IOD oraz do realizowania jego zaleceń przy wykonywaniu zadań dotyczących ochrony danych osobowych;

6) Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub rażące nienależyte wykonanie zobowiązania, w szczególności przez osobę, która wobec naruszenia nie powiadomiła o tym IOD.

§ 9.

1) Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych), stanowi załącznik nr 1 do Polityki.

2) Wykaz zbiorów danych osobowych wraz ze wskazaniem programów komputerowych zastosowanych do przetwarzania danych (w przypadku zbiorów danych prowadzonych w wersji elektronicznej), stanowi załącznik nr 2 do Polityki.

3) Instrukcja zarządzania systemem informatycznym, stanowi załącznik numer 3 do Polityki.

§ 10.

1) Niezależnie od praw i obowiązków, określonych w niniejszej Polityce, przetwarzanie danych osobowych zawartych w dokumentacji medycznej odbywa się w zakresie i zasadach określonych w:

   a) przepisach ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta;
   b) przepisach rozporządzeń Ministra Zdrowia w sprawie rodzajów i zakresu dokumentacji medycznej, sposobu jej przetwarzania oraz wzorów określonych rodzajów dokumentacji medycznej, w szczególności wzoru książeczki zdrowia dziecka, wydanych na podstawie art. 30 ust. 1 ustawy wskazanej w pkt 1;
   c) innych przepisach szczególnych, w tym dotyczących:

- ✓ świadczeń opieki zdrowotnej finansowanych ze środków publicznych,
- ✓ zapobiegania oraz zwalczania zakażeń i chorób zakaźnych u ludzi,
- ✓ chorób zawodowych,
- ✓ medycyny pracy,
- ✓ ubezpieczeń społecznych oraz świadczeń pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa.

2) Przepisy, z ust.1 wskazują w szczególności:

a) Podstawę przetwarzania danych osobowych;

b) Zakres gromadzonych i przetwarzanych danych osobowych;
c) Formę przetwarzania danych osobowych;
d) Podstawę i zakres udostępniania danych osobowych posiadanych przez PL oraz podmiot uprawniony do dostępu do tych danych osobowych;
e) Okres przetwarzania (przechowywania) tych danych osobowych.

§ 11.

Monitoring w Gminnym Ośrodku Zdrowia Trąbki Wielkie Samodzielny Publiczny Zakład Opieki Zdrowotnej.

Monitoring wizyjny jest inwazyjną formą przetwarzania danych osobowych i podlega szczególnej weryfikacji przez Administratora Danych. Ważne jest, aby jego stosowanie było zasadne, zgodne z prawem i nie naruszało ochrony danych osobowych osób monitorowanych. Podstawy przetwarzania danych osobowych to Rozporządzenie 2016/679 określające zasady przetwarzania danych osobowych oraz podstawy umożliwiające ich przetwarzanie (art.6 a w przypadku danych wrażliwych art. 9 i 10 rozporządzenia).

Tabela – Monitoring wizyjny lista kontrolna.

CO WERYFIKUJEMY?	UZASADNIENIE
Czy stosowany jest monitoring w czasie rzeczywistym bez dokonywania zapisu?	Monitoring jest nagrywany. Czas przechowywania 30 dni. Potem jest nadpisywanie, taśmy nie są archiwizowane.
Czy zapis z monitoringu można przeszukiwać według określonych kryteriów (np. czasu, miejsca)?	Tak można przeszukiwać według kryteriów, daty, godziny i miejsca.
Czy zapisywany jest wyłącznie obraz czy również głos?	Zapisywany jest tylko obraz bez głosu.
Jaki rodzaj danych przetwarzany jest przy użyciu monitoringu (dane zwykłe/dane wrażliwe)?	Żadne dane osobowe nie są przetwarzane przy użyciu monitoringu. Jest on używany do zapewnienia bezpieczeństwa pracownikom i pacjentom jak również w celu zabezpieczenia mienia Ośrodka.
Czy zapis z monitoringu można powiązać z innymi informacjami posiadanymi przez dany podmiot (np. księgą wejść, przepustkami, identyfikatorami)?	Nie temu służy monitoring. Nie jest używany do rejestracji wejść czy wyjść, nie służy do sprawdzania listy obecności.
Rozmieszczenie kamer?	Na zewnątrz i wewnątrz budynku.
Na jakim nośniku zapisywane są nagrania?	Na nagrywarce.
Jak długo przechowywane są nagrania?	Nagrywania są przechowywane 30 dni.
Gdzie przechowywane są nagrania?	W pomieszczeniu zabezpieczonym.
W jaki sposób nagrania są usuwane?	Są przez przycisk kasuj usuwane są z nośnika/nagrywarki
Kto i na jakich zasadach może uzyskać dostęp do nagrań?	Do nagrań ma dostęp tylko Administrator i osoba przez niego upoważniona. Nagrania są odtwarzane, jeżeli doszło do zagrożenia życia. Albo

	do wyraźnego zagrożenia bezpieczeństwa (np. kradzież, świadome zniszczenie mienia Ośrodka).
W jaki sposób realizowany jest obowiązek informacyjny?	Obszar objęty monitoringiem jest właściwie oznaczony (piktogramy, tablice), pracownicy są poinformowani o monitoringu, i wiedzą, że nie przekazujemy informacje, o których mowa w art. 24 UODO.

§ 12.

Analiza i szacowanie ryzyk, stanowią załącznik nr 4 niniejszej Polityki.

§ 13.

Rejestr osób upoważnionych do przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 RODO, stanowi załącznik nr 5 do Polityki. Rejestr, ma formę pisemną oraz formę elektroniczną.

§ 14.

Rejestr przypadków udostępnienia danych zawartych w dokumentacji medycznej, o którym mowa w art. 27 ust. 4 ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, stanowi załącznik nr 6 do Polityki. Ma formę pisemną i formę elektroniczną.

§ 15.

Protokół z naruszenia poufności nośnika danych osobowych stanowi załącznik nr 7 do Polityki. Ma formę pisemną i formę elektroniczną.

§ 16.

Raport z naruszenia ochrony danych osobowych stanowi załącznik nr 8 do Polityki. Ma formę pisemną i formę elektroniczną.

§ 17.

Analiza naruszenia danych na podstawie art. 33 ust. 5 RODO stanowi załącznik nr 9. Ma formę pisemną i formę elektroniczną.

§ 18.

Rejestr czynności przetwarzania danych osobowych prowadzony jest w formie elektronicznej – plik exel.