Wojewódzki Specjalistyczny Zespół
Zakładów Opieki Zdrowotnej
Chorób Płuc i Gruźlicy
w Wolicy k/Kalisza

Wojewódzki Specjalistyczny Zespół Zakładów Opieki Zdrowotnej Chorób Płuc i Gruźlicy w Wolicy k/Kalisza

Polityka bezpieczeństwa i ochrony danych osobowych

Niniejszy dokument jest dowodem na zaadoptowanie i spełnianie przez WSZZOZ w Wolicy k/Kalisza wymagań Rozporządzenia Parlamentu Europejskiego i Rady UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) z dnia 27-04-2016 r.

	Stanowisko:	Imię i nazwisko:	Data:	Podpis:
Opracował	Inspektor Ochrony Danych Osobowych	Jacek Gołdych	15.06.2021 r.	INSPEKTOR Ochrony Danych Osobowych Jacek Gołdych
Zatwierdził pod względem formalno – prawnym	Dyrektor WSZZOZ	Sławomir Wysocki	15.06.2021 r.	DYREKTOR Wojewódzkiego Specjalistycznego ZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza lek. med. Sławomir Wysocki

SPIS TREŚCI

I. POLITYKA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH – WYMAGANIA OGÓLNE

Polityka Bezpieczeństwa Danych Osobowych jest dokumentem pełniącym rolę konstytutywną w stosunku do wszystkich innych - wydanych w tym zakresie wewnętrznych zarządzeń, procedur i instrukcji. Uzupełnieniem niniejszego dokumentu są wszelkie regulacje cytowane lub przywoływane w niniejszym dokumencie funkcjonujące w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza dokumenty wewnętrzne tj. procedury, regulaminy itp.

Polityka Bezpieczeństwa Danych Osobowych jest to formalny zapis zasad, według których zobowiązane są postępować osoby, posiadające dostęp do technologii organizacji i do jej zasobów informacyjnych. Polityka odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych przy zachowaniu poufności, integralności, autentyczności, rozliczalności i dostępności informacji, przy niezawodności pracy całości systemu a w szczególności aplikacji i urządzeń zawierających, przetwarzających, przesyłających informacje podlegające ochronie.

Założeni Polityki bezpieczeństwa i Ochrony Danych Osobowych opracowano również na założeniach Kodeksu Postępowania dla Podmiotów Wykonujących Działalność Leczniczą.

Przedmiotem ochrony na podstawie niniejszej Polityki są dane osobowe, agregowane zarówno w systemach informatycznych, jak również na nośnikach papierowych i elektronicznych. Polityka ma zastosowanie do wszystkich danych osobowych przetwarzanych w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza w ramach realizowanych procesów/działań operacyjnych. Obowiązek ochrony danych osobowych przetwarzanych w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza dotyczy wszystkich osób, które mają do nich dostęp bez względu na zajmowane stanowisko oraz miejsce wykonywania pracy, jak również charakter stosunku pracy. Każda osoba, która ma mieć dostęp do danych osobowych, będzie mogła je przetwarzać wyłącznie na podstawie otrzymanego upoważnienia. Osoby mające dostęp do danych osobowych są zobowiązane do zapoznania się z Polityką i innymi powiązanymi z nią dokumentami oraz stosowanie zawartych w nich regulacji. Polityka zachowuje zgodność z innymi wewnętrznymi regulacjami z obszaru bezpieczeństwa informacji i systemów informatycznych obowiązującymi w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza. Nadzór nad opracowaniem i aktualizacją Polityki sprawuje Inspektor Ochrony Danych Osobowych.

II. DEKLARACJA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH

„Deklaracja Dyrekcji WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza dla zachowania bezpieczeństwa i ochrony przetwarzanych danych osobowych w ramach prowadzonej działalności"

WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza mając na uwadze jak ważną funkcji w prowadzonej działalności podmiotu leczniczego pełni ochrona informacji w tym bezpieczeństwo i ochrona danych osobowych przyjmuje niniejsza deklaracje jako kierunek działań dla zapewnienia należytego poziomu jej bezpieczeństwa i ochrony.

Jako Dyrektor WSZZOZ wyznaczam następujące cele naszych działań dla bezpieczeństwa i ochrony przetwarzanych danych w tym danych osobowych:

1. Systematyczną identyfikacje i spełnianie wszelkich wymagań prawnych wymagających od podmiotu leczniczego zapewnienia odpowiedniego poziomu bezpieczeństwa i ochrony informacji,
2. Zapewnienie wsparcia dla inicjatyw z zakresu bezpieczeństwa i ochrony informacji,
3. Zapewnienie zasobów potrzebnych dla wdrażania wymaganych zabezpieczeń,
4. Objęcie szczególnym nadzorem dokumentacji medycznej sporządzanej w ramach udzielanych świadczeń medycznych,
5. Zapewnienie działań na rzecz kształtowania świadomości pracowników co do ważności i rangi przetwarzanych danych w tym danych osobowych.

W imieniu WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza
Sławomir Wysocki – Dyrektor
Wolica 15.06.2021 r.

III. PODSTAWY PRAWNE

Niniejszy dokument został oparty na założeniach wymagań prawnych w zakresie ochrony i bezpieczeństwa danych osobowych jakie każde przedsiębiorstwo przetwarzające dane osobowe zobowiązane jest spełniać między innymi, Rozporządzenie Parlamentu Europejskiego i Rady UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) z dnia 27-04-2016 r.

W opracowaniu niniejszego dokumentu uwzględniono również założenia Kodeksu Postępowania dla podmiotów wykonujących działalność lecznicza jako promowanego przez środowiska medyczne i prawnicze standardu postępowania.

IV. TERMINOLOGIA

1. **Rozporządzenie** - 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.

2. **Administrator Danych Osobowych = ADO** - Zgodnie z definicją RODO administrator danych osobowych oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych = WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza.
3. **Dane osobowe** - oznaczają 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.
4. **Szczególne kategorie danych osobowych** – 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.
5. **Inspektor Ochrony Danych Osobowych** - Osoba wyznaczona przez Administratora Danych na podstawie art. 37 RODO, która realizuje zadania monitorowania przestrzegania przepisów o ochronie danych osobowych w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza określone w art. 39 RODO.

V. ODPOWIEDZIALNOŚĆ

1. Administrator Danych Osobowych

Administratorem Danych Osobowych jest osoba decydująca o celach i środkach przetwarzania danych osobowych, którą jest WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza. W imieniu ADO stroną reprezentująca jest Dyrektor zgodnie z zapisami Księgi Rejestrowej oraz statutu Zakładu. Administrator Danych Osobowych odpowiada za zapewnienie technicznych i organizacyjnych warunków dla bezpieczeństwa przetwarzanych danych osobowych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności za bezpieczeństwo danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, utratą, uszkodzeniem, lub zniszczeniem.

<u>Do zadań ADO należy:</u>

1. Nadzór zachowania „szczególnej staranności" oraz przestrzeganie zasad:

1.1. Legalności przetwarzania danych osobowych będących w posiadaniu podmiotu,

1.2. Niezmieniania celu przetwarzania danych,

1.3. Merytorycznej poprawności danych oraz ich adekwatności w stosunku do celów, w jakim dane te są przetwarzane,

1.4. Czasowego przetwarzania danych (nie dłużej, niż jest to niezbędne do realizacji celu ich przetwarzania),

2. Administrator zobowiązany jest do informowania podmiotu, którego dane dotyczą – każdorazowo na wniosek zainteresowanego/ osoby fizycznej.

3. Powoływanie i odwoływanie w drodze zarządzeń Inspektora Ochrony Danych Osobowych oraz Administratora Systemu Informatycznego.
4. Podejmowania decyzji o zakupie, modernizacji, wymianie wszelkich rozwiązań technicznych i technologicznych zapewniających bezpieczne przetwarzania danych osobowych na wniosek IODO i ASI (odpowiednio do stopnia eksploatacji, poziomu gwarantowanego bezpieczeństwa, aktualnych rozwiązań technicznych).
5. Zatwierdzanie pod względem formalno – prawnym wszystkich dokumentów w ramach polityki bezpieczeństwa.

2. Inspektor Ochrony Danych Osobowych (IODO)

W związku z prawnym aspektem co do kryteriów konieczności wyznaczania Inspektora Ochrony Danych Osobowych – Art 37 RODO, decyzją Administratora Danych Osobowych, funkcja ta została powierzona w drodze Zarządzenia Dyrektora WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza. Szczegółowy zakres zadań odpowiedzialności i uprawnień Inspektora ochrony Danych Osobowych wyspecyfikowano w załączniku Nr 1 do uprzednio cytowanego zarządzenia.

3. Administrator Systemu Informatycznego (ASI)

Administrator Danych Osobowych w drodze decyzji, odpowiednio do zapisów zawartej umowy o współpracy, powołał Administratora Systemu Informatycznego odpowiedzialnego za całokształt działań w ramach poprawności funkcjonowania i zapewnienia właściwego poziomu bezpieczeństwa systemu informatycznego.

Do zadań Administratora Systemu Informatycznego w zakresie ochrony danych osobowych w ramach powierzonej funkcji należy:

1. koordynacja wdrażania i monitorowanie działań w ramach wdrożonych zabezpieczeń technicznych i organizacyjnych, mających na celu ochronę przetwarzania danych osobowych w systemach informatycznych,
2. Przydzielanie praw dostępu do przetwarzania danych osobowych w systemie informatycznym dla pracowników i/ lub osób stale współpracujących z WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza, na podstawie indywidualnych upoważnień,
3. Monitorowanie i analiza stanu sprzętu i urządzeń technicznych przetwarzających dane osobowe, bieżąca ich modernizacja zgodnie z rozwojem techniki adekwatnie do rodzaju wykorzystywanego sprzętu,
4. Zabezpieczenie urządzeń, dysków lub innych nośników informatycznych, zawierających dane osobowe, przeznaczonych do likwidacji, tak by uprzednio były pozbawione zapisu tych danych, a w przypadku, gdy nie jest to możliwe - zostały uszkodzone w sposób uniemożliwiający ich odczytanie,
5. Zabezpieczenie urządzeń, dysków lub innych nośników informatycznych, zawierających dane osobowe, przeznaczonych do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, tak aby były uprzednio pozbawione zapisu danych, a w przypadku, gdy nie jest to możliwe - zostały uszkodzone w sposób uniemożliwiający ich odczytanie,

6. Zabezpieczenie urządzeń, dysków lub innych nośników informatycznych, zawierających dane osobowe, przeznaczonych do naprawy, tak aby zostały uprzednio pozbawione zapisu tych danych, a gdy jest to niemożliwe - aby były naprawione pod nadzorem osoby upoważnionej,
7. Analiza informowanie kierowników jednostek organizacyjnych o przekroczeniu uprawnień, naruszeniu zasad bezpieczeństwa obowiązujących przy przetwarzaniu danych osobowych,
8. Prowadzenie szkoleń dla pracowników przetwarzających dane osobowe w systemie informatycznym,
9. Stała współpraca z Administratorem danych Osobowych oraz Inspektorem Ochrony Danych Osobowych w zakresie bezpieczeństwa i ochrony danych osobowych,

W celu realizacji powierzonych zadań Administrator Systemu Informatycznego w zakresie ochrony danych osobowych ma prawo:

1. kontrolować komórki organizacyjne/ stanowiska w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza pod kątem właściwego zabezpieczenia danych osobowych w przetwarzanych w systemie informatycznym,
2. informować Dyrektora/Administratora Danych Osobowych oraz Inspektora Ochrony Danych Osobowych w przypadkach naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,

Administrator Systemu Informatycznego w zakresie ochrony danych osobowych ma obowiązek sprawdzenia czy naruszenie zasad ochrony danych osobowych nastąpiło z winy pracownika i/ lub osoby stale współpracującej z WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza oraz zabezpieczenia materiałów niezbędnych do wyjaśnienia sprawy,

Jeżeli zachodzi podejrzenie, że naruszenie lub zagrożenie bezpieczeństwa ochrony danych osobowych jest wynikiem przestępstwa, Administrator Systemu Informatycznego w zakresie ochrony danych osobowych w porozumieniu z Dyrektora/Administratora Danych Osobowych oraz Inspektorem Ochrony Danych Osobowych zawiadamia o powyższych okolicznościach właściwe organy.

4. Kadra kierownicza na poziomie operacyjnym

Kadra kierownicza WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza stanowi niezwykle ważny obszar w strukturze organizacyjnej w aspekcie właściwego wdrożenia i funkcjonowania zasad ustanowionej polityki bezpieczeństwa i ochrony danych osobowych. Do zadań kadry kierowniczej w aspekcie poprawności i prawidłowości funkcjonowania przyjętej Polityki należy:

1. Bieżący nadzór i kontrolę przestrzegania zasad przyjętych w niniejszym dokumencie oraz dokumentacji systemu zarządzania jakością regulujące zasady postępowania w zakresie bezpieczeństwa informacji w tym ochrony danych osobowych,
2. Reagowanie na wszelkie nieprawidłowości w zakresie bezpieczeństwa informacji w tym ochrony danych osobowych w podległym im obszarze,
3. Zgłaszanie wszelkich informacji/ zdarzeń itp. związanych w bezpieczeństwem informacji i ochroną danych osobowych w odniesieniu do podległego im obszaru do Inspektora Ochrony Danych Osobowych opcjonalnie Dyrektora WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza,

4. Zgłaszanie pomysłów, wniosków racjonalizatorskich których celem będzie poprawa bezpieczeństwa informacji w tym ochrony danych osobowych.

5. Pracownicy/osoby współpracujące z WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza

Pracownicy/osoby współpracujące z WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza posiadający stosowane upoważnienia do przetwarzania danych osobowych oraz dostęp do zbiorów danych osobowych mają obowiązek przestrzegania postanowień dokumentu Polityki Bezpieczeństwa oraz szczegółowych procedur postępowania w tym również, przepisów prawa regulujących kwestie bezpieczeństwa i ochrony przetwarzanych danych osobowych. Użytkownik systemu informatycznego ma prawo do wykonywania tylko tych czynności, do których został upoważniony. Użytkownik systemu ponosi wszelką odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień, traktowane będą, jako naruszenie podstawowych obowiązków pracowniczych lub naruszenie zapisów umowy. Każdy pracownik/ osoba współpracująca z WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza wykonująca zadania związane z przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały przekazane osobom nieuprawnionym lub nie zostały użyte w sposób niezgodny z ich przeznaczeniem.

VI. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

Przetwarzanie danych osobowych jest zgodne z prawem krajowym/Unijnym wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

Szczegółowe zasady przetwarzania danych osobowych regulują odpowiednie przepisy prawa. Administrator Danych Osobowych zobowiązany jest do bieżącego śledzenia aktualności wymagań prawnych (we współpracy z osobami odpowiedzialnymi za poszczególne obszary w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza w ramach, których przetwarzane są dane osobowe) oraz terminowe

informowanie Administratora i Inspektora Ochrony Danych Osobowych o pojawiających się zmianach i wynikających z nich potrzebach.

Każdorazowo o ile nie istnieją prawne przesłanki do przetwarzania danych osobowych jako warunek niezbędny/ konieczny do zrealizowania usługi lub w obszarze administracyjno – organizacyjnym WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza Administrator Danych Osobowych zobowiązany jest dopełnić należytych starań, aby uprzednio przed podjęciem realizacji usługi, pozyskać od osób fizycznych, których dane będę przetwarzane oświadczenie zgody. Szczegółowo kwestie związane z pozyskaniem i zabezpieczaniem dowodu zgody na przetwarzanie danych osobowych reguluje ***Procedura – zasady przetwarzania/ archiwizowania dokumentu wyrażonej zgody na przetwarzanie danych osobowych***.

VII. RODZAJE PRZETWARZANYCH DANYCH OSOBOWYCH

WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza w zakresie prowadzonej działalności/prowadzonych działań operacyjnych przetwarza dane osobowe:

a) Pracowników/ osoby współpracujące z WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza,
b) Klientów/ pacjentów korzystających z usług medycznych WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza w poszczególnych obszarach,
c) Opiekunów faktycznych i prawnych w ramach realizowanych usług medycznych,
d) Kontrahentów w ramach prowadzonej współpracy

W większości przypadku prowadzonych działań operacyjnych WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza przetwarza szczególne kategorie danych (zgodnie z Art. 9 RODO = dane o stanie zdrowia/ zrealizowanych świadczeniach medycznych).

Administrator Danych Osobowych we współpracy z Inspektorem Ochrony Danych osobowych każdorazowo przed podjęciem nowych działań operacyjnych/ dotychczas nie realizowanych których specyfika związana jest z przetwarzaniem danych osobowych zobowiązany jest dokonać szczegółowej analizy kategorii osób których dane będą przetwarzane jak i zakresu i rodzaju danych tak aby właściwie oszacować potencjalne ryzyko związane z niniejszymi operacjami i wdrożyć właściwe środki zaradcze gwarantujące odpowiedni poziom ochrony i bezpieczeństwa danych.

VIII. ORGANIZACJA DZIAŁAŃ W WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza W RAMACH PRZETWARZANIA DANYCH OSOBOWYCH

Dane osobowe przetwarzane w ramach realizowanych procesów/ działań operacyjnych w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza dotyczą organizacji i udzielania świadczeń medycznych.

W przypadku konieczności pozyskania zgody od osób których dane osobowe będą przetwarzane Administrator Danych Osobowych decyduje o kształcie klauzuli zgody jak i o obowiązku informacyjnym ciążącym na nim w tej sytuacji.

IX. WARUNKI WYRAŻENIA ZGODY

Wszędzie tam, gdzie specyfika realizowanych zadań operacyjnych wymaga pozyskiwanie i przetwarzania danych osobowych i niej spełnione są przesłanki do przetwarzania niniejszych danych na podstawie litery prawa, umowy czy prawnie uzasadnionego interesu Administratora pozyskiwana jest zgoda na przetwarzanie danych osobowych. 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. Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

X. INFORMACJE PODAWANE W PRZYPADKU ZBIERANIA DANYCH OD OSOBY KTÓREJ DANE DOTYCZĄ

Administrator Danych Osobowych zobligowany jest do publikowania danych w ramach tzw. obowiązku informacyjnego wszędzie tam, gdzie przetwarzanie odbywa się na podstawie wyrażonej zgody. Z chwilą wystandaryzowania wzoru klauzuli zgody Administrator Danych Osobowych określa treść obowiązku informacyjnego jak również podejmuje decyzję co do formy jego publikacji.

Podobnie jak wzór klauzuli zgody, treść obowiązku informacyjnego podlega okresowej weryfikacji i aktualizacji przez Administratora Danych Osobowych. Niezależnie od powyższego dla zagwarantowania poprawności działania jak i rzetelności przetwarzania danych osobowych Administrator Danych Osobowych publikuje za pośrednictwem strony internetowej WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza w zakładce kontakt // „dane osobowe" podstawowy zakres informacji w ramach procesu przetwarzania danych osobowych. Za nadzór i koordynację działań w ramach poprawności publikowanych informacji na stronie internetowej WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza odpowiada Inspektor Ochrony Danych Osobowych we współpracy z Administratorem Systemu Informatycznego.

XI. PRAWA OSÓB KTÓRYCH DANE SA PRZETWARZANE I ZASADY ICH RESPEKTOWANIA

Administrator Danych Osobowych zobowiązany jest zapewnić pełna możliwość respektowania praw osób których dane osobowe są przetwarzane w tym między innymi:

- Prawo dostępu przysługujące osobie, której dane dotyczą (uzyskiwania informacji) (Art. 15 RODO)
- Prawo do sprostowania danych (Art. 16 RODO)
- Prawo do usunięcia danych („prawo do bycia zapomnianym") – (Art. 17 RODO)
- Prawo do ograniczenia przetwarzania (Art. 18 RODO)
- Prawo do przenoszenia danych (Art. 20 RODO)
- Prawo sprzeciwu (Art. 21 RODO)

Każdorazowo w ramach zgłoszenia się do WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza osoby z żądaniem prawa w zakresie przetwarzanych danych dotyczących jego osoby, pracownik odbierający takowa informację zobowiązany jest:

- właściwie ją odnotować,
- niezwłocznie przekazać do ADO i/lub do Inspektora Ochrony Danych Osobowych.
- podjąć działania informacyjne, aktualizacyjne lub inne w zależności od żądania osoby wnioskującej.

W przypadku zaistnienia sytuacji, kiedy przepis innego aktu prawnego stanowi inaczej tj. zakłada dalej idącą ochroną lub wymóg archiwizacji, zastosowanie mają niniejsze przepisy prawa, co jednocześnie nie zwalnia ADO z obowiązku udzielenia stosownej informacji. Administrator Danych Osobowych zobowiązany jest do przedłożenia/przesłania osobie wnioskującej stosownej odpowiedzi. W sytuacji powierzania danych podmiotom przetwarzającym lub udostępniania danych innym administratorom danych należy ich powiadamiać o każdym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, które było wynikiem realizacji wniosku otrzymanego od osoby, której dane dotyczą. Osobą odpowiedziała za właściwe zredagowanie pisma, jak również archiwizację i nadzór w tym zakresie sprawuje Inspektor Ochrony Danych Osobowych.

XII. POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

Jeżeli przetwarzanie ma być dokonywane w imieniu Administratora Danych Osobowych, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia ogólnego i chroniło prawa osób, których dane dotyczą. O wyborze podmiotu spełniającego wymagane kryteria poprawności i bezpieczeństwa przetwarzania decyduje Administrator Danych Osobowych. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje Administratora Danych Osobowych o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też

przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny,

b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

c) podejmuje wszelkie środki gwarantujące należyty poziom bezpieczeństwa i ochrony przetwarzanych danych osobowych.

Szczegółowe zasady postępowania w ramach zawierania, archiwizacji i monitorowania poprawności realizacji zadań w ramach umowy powierzenia określa ***Procedura PO-5 – zasady powierzania przetwarzania danych osobowych.***

XIII. REJEST CZYNNOŚCI PRZETWARZANIA

Administrator Danych Osobowych zobowiązany jest odpowiednio do wymagań prawnych Rozporządzenia do prowadzenia rejestru czynności przetwarzania danych osobowych. Niniejszy rejestr sporządzany jest w oparciu o szczegółową inwentaryzację procesów/ działań operacyjnych i przetwarzanych w nich danych osobowych. Rejestr prowadzony jest w wersji elektronicznej, pod nadzorem Inspektora Ochrony Danych osobowych, podlega bieżącej aktualizacji każdorazowo o ile wystąpią jakiekolwiek zmiany w zakresie prowadzonych działań operacyjnych i przetwarzanych w nich danych osobowych.

Rejestr czynności przetwarzania udostępniany jest każdorazowo na żądanie organu nadzorczego. W innych sytuacjach decyzję co do udostepnienia rejestru operacji podejmuje Administrator Danych Osobowych. Z uwagi na istotność danych zawartych w rejestrze dla działalności WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza jak i ustanowionej Polityki jest on zabezpieczony przed nieautoryzowaną zmianą, modyfikacją itp.

XIV. ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Incydent związany z bezpieczeństwem informacji - to pojedyncze zdarzenie lub seria zdarzeń niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji, w tym danych osobowych. Szczegółowo zasady postepowania w ramach wystąpienia incydentu naruszenia bezpieczeństwa i ochrony danych osobowych reguluje ***Procedura PO – 5 zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa przetwarzania danych osobowych.***

XV. DOBÓR ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH DOTYCZĄCYCH PRZETWARZANIA I ZABEZPIECZANIA DANYCH OSOBOWYCH

Dobór środków technicznych i organizacyjnych dotyczących przetwarzania i zabezpieczania danych osobowych w Zakładzie realizowany jest w oparciu o szacowanie ryzyka naruszenia praw i wolności osób, których dane dotyczą. Zasady dotyczące przeprowadzania szacowania ryzyka naruszenia

praw i wolności osoby fizycznej określone zostały w Rozdziale XVI niniejszej Polityki. Przy doborze zabezpieczeń należy i oceniać ryzyko zarówno w kontekście skutków dla osoby, której dane dotyczą w tym np. dyskryminacja, pozbawienie przysługujących praw, szkody majątkowe i niemajątkowe), jak również ryzyko w kontekście skutków dla WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza w przypadku niepodjęcia działań związanych zapewnienie przetwarzania danych osobowych zgodnie z RODO. Dobór zabezpieczeń dla systemów informatycznych wykorzystywanych do przetwarzania danych następuje na podstawie procedur szacowania ryzyka przyjętych w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza w tym również rekomendacji Administratora Systemu Informatycznego zakresie możliwych do zastosowania rozwiązań technicznych. Ustalone wymagania dotyczące zabezpieczenia danych osobowych w odniesieniu do danego procesu przetwarzania danych osobowych są odnotowywane przez Inspektora Ochrony Danych w prowadzonym rejestrze czynności przetwarzania danych osobowych. Planowanie realizacji nowych procesów związanych z przetwarzaniem danych osobowych, w tym w szczególności nowych systemów informatycznych służących do przetwarzania danych osobowych, musi uwzględniać zasady ochrony danych w fazie projektowania („privacy by design") oraz domyślnej ochrony danych („privacy by default").

Projektowanie nowych usług związanych z przetwarzaniem danych osobowych wspieranych przez systemy informatyczne odbywa się w ramach bieżących działań operacyjnych prowadzonych przez Dyrektora we współpracy z pracownikami operacyjnymi oraz Administratorem Systemu Informatycznego. W przypadku realizacji procesów przetwarzania danych osobowych w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem przetwarzania należy dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych zgodnie z art. 35 RODO. Jeżeli dokonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby nie zostały zastosowane środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania należy skonsultować się z krajowym organem nadzoru ochrony danych osobowych. W przypadku konieczności przeprowadzenia konsultacji z organem nadzorczym Inspektor Ochrony Danych Osobowych przygotowuje odpowiedni wniosek o konsultacje zgodnie z art. 36 RODO i kontaktuje się w tej sprawie z organem.

XVI. ANALIZA RYZYKA DLA OPERACJI NA DNAYCH OSOBOWYCH

Z uwagi, iż WSZZOZ wykorzystuje w ramach ustanowionej polityki bezpieczeństwa i ochrony danych osobowych założenia Normy PN-EN- ISO/IEC 27001:2014, szacowanie i ocenę ryzyka w tym ocenę skutków dla operacji związanych z przetwarzaniem danych osobowych przeprowadzono zgodnie z przyjętą metodyką.