POLITYKA

BEZPIECZEŃSTWA DANYCH

OSOBOWYCH

Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie

ul. Pstrowskiego 28B

10-602 Olsztyn

Data wprowadzenia:	**07. 05. 2008**
Wersja:	**4**
Daty aktualizacji:	**30. 04. 2021**
Zarządzenie Dyrektora	**17/2021 z dnia 30.04.2021**
Opracował:	**Jolanta Janiszewska** Inspektor Ochrony Danych
Zatwierdził:	**Marek Myszkowski** Dyrektor

SPIS TREŚCI

A. INFORMACJE OGÓLNE

1. CEL POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Celem niniejszej Polityki jest spełnienie wymagań określonych w Rozporządzeniu 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.

Polityka bezpieczeństwa danych osobowych ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce bezpieczeństwa danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Ponadto, celem wprowadzenia dokumentu jest szczegółowe określenie środków technicznych i organizacyjnych, procedur, zasad i regulacji wewnętrznych które zapewnią przetwarzania danych osobowych w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie (dalej zwana WSPR) w sposób zgodny z prawem, bezpieczny, chroniący przed ich udostępnieniem osobom nieupoważnionym, utratą, uszkodzeniem lub zniszczeniem.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

2. TERMINOLOGIA

1. **Administrator Danych (ADO)** – podmiot decydujący o celach, sposobach i środkach przetwarzania danych osobowych tj. Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie (WSPR).
2. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych,
3. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, 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. **Dane służbowe** - dane osobowe pracowników lub współpracowników służące do kontaktowania się z nimi w sprawach służbowych, tj. imię i nazwisko, stanowisko służbowe (zawód), służbowy numer telefonu, służbowy adres e-mail, ewentualnie informacje związane ze stanowiskiem służbowym (np. godziny pracy, miejsce pracy).
5. **Dane wrażliwe** - zgodnie z art. 27 ust.1 Ustawy o ochronie danych osobowych jest to zamknięty katalog do którego należą: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, dane genetyczne, nałogach lub życiu seksualnym, dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
6. **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
7. **Identyfikator użytkownika** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie.
8. **Informatyk** - osoba odpowiedzialna za bezpieczeństwo danych przetwarzanych w systemach informatycznych.
9. **Odbiorca danych** - każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby upoważnionej do przetwarzania danych,

c) podmiotu, któremu powierzono przetwarzanie danych osobowych

d) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w

związku z prowadzonym postępowaniem.

10. **Organ nadzorczy** – niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO,

11. **Państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.

12. **Podmiot przetwarzający** –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych.

13. **Polityka bezpieczeństwa** – niniejsza Polityka bezpieczeństwa danych osobowych.

14. **Powierzenie przetwarzania danych** - zlecenie wykonania czynności przetwarzania danych innemu podmiotowi, w drodze odrębnej umowy zawartej na piśmie (umowa powierzenia) lub stosownego zapisu do umowy, wyłącznie w zakresie i celu w niej przewidzianym.

15. **Pracownik** – osoba zatrudniona na podstawie stosunku pracy. Ilekroć w Polityce jest mowa o pracowniku, należy przez to rozumieć także osoby wykonujące zadania i/lub prace w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie, niezależnie od rodzaju stosunku formalnego łączącego tę osobę z WSPR (np. umowa zlecenie, o dzieło, kontrakt, staż, specjalizacja, praktyka, wolontariat etc.).

16. **Procesor** - podmiot, z którym Administrator danych zawarł umowę powierzenia.

17. **Przetwarzanie danych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.

18. **Rejestr przetwarzania danych** - wewnętrzny firmowy dokument, prowadzony w formie elektronicznej oraz w formie dokumentu papierowego. Jest to dokument, który ma pokazywać w szczególności w jakich procesach w organizacji są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczane. Dokument ten będzie musiał zostać udostępniony na każde wezwanie GIODO.

19. **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

20. **RODO** – Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych).

21. **Udostępnianie danych** - przekazanie danych poza organizację. Udostępnienie danych osobowych osobom trzecim jest dopuszczalne na gruncie przepisów Rozporządzania RODO m.in. na podstawie art. 6 i 9, przy czym należy zachować wszelkie procedury, aby udostępnienie danych osobowych osobom trzecim było zgodne z przepisami. Niezbędne jest sprawdzenie podstawy prawnej do udostępnienia danych osobowych, zweryfikowanie osoby trzeciej, której udostępniane są dane osobowe, ale także prowadzenie rejestru udostępnień.

22. **Unia** – Unia Europejska,

23. **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.).

24. **Usuwanie danych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (anonimizacja danych), dokonane w sposób trwały, tj. bez możliwości ich odzyskania (np. za pomocą dedykowanego systemu do bezpiecznego usuwania danych, demagnetyzacja, zniszczenie fizyczne nośnika danych.

25. **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES ZASTOSOWANIA

Polityka bezpieczeństwa danych osobowych opisuje zasady i procedury zarządzania systemem chroniącym dane oraz sposoby reagowania na zagrożenia. Jest to zestaw praw I reguł dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie.

Polityka odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Politykę bezpieczeństwa danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

Rygorowi Polityki podlegają także dane powierzone Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały jej udostępnione.

Stosowanie niniejszej Polityki Bezpieczeństwa Danych Osobowych ma na celu zapewnienie zabezpieczenia adekwatnego i proporcjonalnego do kategorii danych, jednocześnie dopasowane do poziomu zagrożeń występujących dla przetwarzanych i przechowywanych danych osobowych w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie.

Przyjęta Polityka Bezpieczeństwa Danych Osobowych powinna być rozwijana w sposób ciągły i zmieniać się wraz ze zmianami w strukturze organizacyjnej, pojawianiem się nowych zagrożeń i zmian wynikających z szacowania ryzyka w bezpieczeństwie informacji WSPR a także rozwojem dostępnych środków zapobiegawczych.

Politykę Bezpieczeństwa Danych Osobowych powinni stosować wszystkie osoby realizujący zadania w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie.

B. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

1. STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie , odpowiadają:

1. Dyrektor Wojewódzkiej Stacji Pogotowia Ratunkowego,
2. Inspektor Ochrony Danych,
3. Informatyk,
4. Bezpośredni przełożeni osób przetwarzających dane osobowe.
5. Każdy pracownik WSPR w Olsztynie, który uzyskał upoważnienie do przetwarzania danych osobowych.

1.1. ADMINISTRATOR DANYCH

1. Administratorem Danych Osobowych jest Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie reprezentowana przez Dyrektora WSPR.
2. Dyrektor jest odpowiedzialny za:
   - zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
   - podejmowanie decyzji o celach, sposobach i środkach przetwarzania danych osobowych,
   - wyznaczeniu Inspektora Ochrony Danych,
   - wdrożenie odpowiednich procedur ochrony danych osobowych,
   - zapewnienie środków umożliwiających prawidłowa realizację praw osób, których dane dotyczą,
   - współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,

- ❖ wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
- ❖ zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
- ❖ dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,
- ❖ zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym,
- ❖ nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, wzór upoważnienia do przetwarzania danych stanowi załącznik nr 1 do Polityki,
- ❖ zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,

<u>w stosunku do IOD:</u>

- zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
- wspieranie IOD w wypełnianiu przez niego zadań, 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,
- zagwarantowanie by IOD nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,
- publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.

3. Administrator Danych wspólnie z IOD opracowują sposoby wykonywania obowiązków wynikających z Polityki.

4. Administrator Danych każdorazowo wyraża zgodę oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania IOD, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.

1.2. INSPEKTOR OCHRONY DANYCH

1. Funkcję Inspektora Ochrony Danych pełni osoba upoważniona przez Administratora Danych.

2. Do zadań IOD należy:
   - ❖ informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,
   - ❖ przygotowywanie upoważnień do przetwarzania danych osobowych,
   - ❖ monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,
   - ❖ monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,
   - ❖ doradztwo w zakresie podziału obowiązków (np. między współadministratorami, Administratorem Danych a podmiotem przetwarzającym lub pomiędzy pracownikami Administratora Danych),
   - ❖ działania zwiększające świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur,
   - ❖ szkolenia dla pracowników Administratora Danych uczestniczących w operacjach przetwarzania danych,
   - ❖ przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,
   - ❖ udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,
   - ❖ współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,
   - ❖ pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.
   - ❖ prowadzenie rejestru czynności przetwarzania danych osobowych, co stanowi załącznik nr 7 do Polityki
   - ❖ prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora, co stanowi załącznik nr 8 do Polityki.
   - ❖ prowadzenie ewidencji zawartych umów powierzenia co stanowi załącznik nr 9 do Polityki.

1.3. INFORMATYK

1. Do zadań Informatyka należy:
   - ❖ prowadzenie ewidencji nadanych uprawnień do systemów informatycznych, co stanowi załącznik nr 5 do Polityki
   - ❖ opracowywanie oraz aktualizacja Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w WSPR,
   - ❖ nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   - ❖ podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
   - ❖ identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
   - ❖ sprawowanie nadzoru nad kopiami zapasowymi;
   - ❖ inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
   - ❖ podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,
   - ❖ dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów,
   - ❖ współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

1.4. BEZPOŚREDNI PRZEŁOŻENI OSÓB PRZETWARZAJĄCYCH DANE

1. Do zadań bezpośrednich przełożonych należy:
   - Przygotowanie wniosku o nadanie upoważnienia do przetwarzania danych osobowych co stanowi załącznik nr 2 do Polityki oraz nadzór nad aktualnością uprawnień posiadanych przez podległych pracowników,
   - Bieżący nadzór nad stosowaniem zabezpieczeń technicznych i organizacyjnych w nadzorowanej sekcji, w szczególności nad przestrzeganiem zasady czystego biurka oraz czystego ekranu,
   - Bieżące zarządzanie danymi osobowymi przetwarzanymi przez osoby podległe,
   - Bieżący nadzór nad pracą w systemie informatycznym pracowników danej komórki organizacyjnej WSPR,
   - Nadzór nad przestrzeganiem polityki bezpieczeństwa danych osobowych, instrukcji teleinformatycznej oraz pozostałych wytycznych dotyczących bezpieczeństwa przetwarzania danych,
   - Delegowanie na szkolenia z zakresu przetwarzania danych osobowych pracowników danej komórki organizacyjnej,
   - Umożliwienie Inspektorowi Ochrony Danych przeprowadzenia kontroli oraz stosowanie się do zaleceń pokontrolnych,
   - Zgłaszanie Inspektorowi Ochrony Danych każdego wykrytego przypadku naruszeń bezpieczeństwa danych osobowych,
   - Kierowanie do Inspektora ochrony Danych informacji o zamiarze tworzenia nowego zbioru danych osobowych, poszerzania zakresu istniejącego zbioru danych osobowych, wdrożenia nowej aplikacji służącej do przetwarzania danych osobowych lub modyfikacji istniejącej aplikacji mogącej mieć wpływ na przetwarzanie danych osobowych,
   - Przekazywanie Inspektorowi Ochrony Danych wszelkich zapytań dotyczących danych osobowych kierowanych przez podmioty zewnętrzne, chyba że zapytanie dotyczy kwestii uregulowanych w innych dokumentach,
   - Inne czynności, opisane w niniejszym dokumencie oraz Instrukcji zarządzania systemem informatycznym obowiązującym w WSPR.

1.5. KAŻDY PRACOWNIK WSPR KTÓRY UZYSKAŁ UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do zadań pracownika który uzyskał upoważnienie do przetwarzania danych osobowych należy:

- Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy, postanowieniami Polityki oraz dokumentami wewnętrznymi regulującymi proces przetwarzania danych osobowych.
- Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w załączniku nr 3 do Polityki.
- Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 108 ze zm.), bądź rozwiązania stosunku cywilnoprawnego.
- Informowanie Inspektora Ochrony Danych i bezpośredniego przełożonego o zaistniałych nieprawidłowościach związanych z przetwarzaniem danych osobowych, jakie wystąpiły na stanowisku pracy tej osoby lub w jej obszarze przetwarzania danych,
- Uczestniczeniu w szkoleniach w zakresie ochrony danych osobowych,
- Inne czynności, opisane w niniejszym dokumencie oraz Instrukcji zarządzania systemem informatycznym obowiązującym w WSPR.

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:
   - zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (*zasada legalności*),
   - w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (*zasada rzetelności*),
   - w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),
   - w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),
   - w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (*zasada minimalizacji danych*),
   - przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),
   - przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (*zasada ograniczenia przechowywania*),
   - w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).
2. Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.
3. Zasady nadawania, zmiany oraz odwołania upoważnień opisane są w załączniku nr 6 do Polityki

2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Wojewódzką Stację Pogotowia Ratunkowego w Olsztynie, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.
2. Obszar przetwarzania danych osobowych w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie stanowi złącznik nr 11 do Polityki
3. Wykaz zbiorów danych osobowych, których administratorem jest Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie oraz procesów przetwarzania zachodzących w tych zbiorach stanowi załącznik nr 12 do Polityki
4. Schemat przepływu danych pomiędzy systemami informatycznymi opisany jest w załączniku nr 13 do Polityki
5. Struktury zbiorów danych osobowych przetwarzanych w Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie stanowi załącznik nr 14 do Polityki

6. Inspektor Ochrony Danych prowadzi:

❖ rejestr czynności przetwarzania danych osobowych, w którym zawarte są następujące informacje:

- nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,
- imię i nazwisko oraz dane kontaktowe IOD,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą,
- opis kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
- gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

- ❖ rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.
  - nazwę oraz dane kontaktowe Administratora Danych,
  - nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,
  - gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,
  - kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
  - gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
  - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

7. Inspektor Ochrony Danych prowadzi rejestry, o których mowa w pkt 3 w formie elektronicznej
8. W przypadku zgłoszenia przez organ nadzoru żądania w tym zakresie, Administrator Danych udostępnia mu prowadzone przez Inspektora Ochrony Danych rejestry.

3. DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.
3. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.
4. Administrator Danych prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi załącznik nr 4 do Polityki.
5. Szczegółowa Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych stanowi załącznik nr 23 do Polityki.

4. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3. Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
   - ❖ przedmiot powierzenia,
   - ❖ czas trwania powierzenia,
   - ❖ charakter i cel przetwarzania,
   - ❖ rodzaj powierzanych danych osobowych,
   - ❖ kategorie osób, których dane dotyczą,
   - ❖ warunki podpowierzenia przetwarzania danych
   - ❖ obowiązki i prawa Administratora Danych,
   - ❖ obowiązki podmiotu przetwarzającego.
4. Właściwą formą zawarcia umowy powierzenia z Wojewódzką Stacją Pogotowia Ratunkowego w Olsztynie jest forma pisemna, wzór umowy powierzenia stanowi załącznik nr 17 do Polityki
5. W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w pkt 3 znajdują się już w zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
6. Za zawieranie umów powierzenia przetwarzania danych osobowych odpowiadają Kierownicy sekcji w których zachodzi potrzeba zawarcia umowy powierzenia przetwarzania danych osobowych.
7. Kierownicy sekcji przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez IOD.
8. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Wojewódzkiej Stacji Pogotowia Ratunkowego lub udzielonymi pełnomocnictwami.

9. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.
10. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.
11. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

5. UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
3. Wniosek o udostępnienie danych musi być złożony na piśmie, co stanowi załącznik nr 19 do Polityki
4. Udostępnienie dokumentacji medycznej realizowane jest na podstawie pisemnego wniosku osoby której dane dotyczą, załącznik nr 21 do Polityki. W przypadku braku możliwości odbioru dokumentacji medycznej osobiście, osoba, której dane dotyczą może upoważnić inną osobę, wypełniając stosowne upoważnienie co stanowi załącznik nr 22 do Polityki.
5. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.
6. Przekazanie przetwarzania danych osobowych podmiotom zewnętrznym, może odbywać się wyłącznie na podstawie pisemnej umowy lub stosownej klauzuli powierzenia, zawartej w umowie łączącej Wojewódzką Stację Pogotowia Ratunkowego w Olsztynie z danym podmiotem. Procesor może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

6. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

1. Przekazywanie danych, których administratorem jest Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.
2. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów 4 i 5 Polityki.
3. Przekazanie danych osobowych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.
4. W przypadku braku decyzji KE, administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.
5. Przekazanie danych może odbyć się wyłącznie na podstawie warunków i postanowień zaakceptowanych przez IOD.

7. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

1. Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2. Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator Danych oraz co najmniej jeden inny podmiot muszą:
   - ❖ być administratorami w rozumieniu art. 4 pkt 7 RODO,
   - ❖ muszą wspólnie ustalić cele przetwarzania danych,
   - ❖ muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.
3. W przypadku spełnienia warunków, o których mowa w pkt 2 Administrator Danych oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.
4. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

8. AUDYTY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie przeprowadzane są przez IOD.
2. IOD przeprowadza audyty wewnętrzne we wszystkich sekcja WSPR w Olsztynie według opracowanego planu audytów.
2. IOD przygotowuje plan audytów na okres nie krótszy niż kwartał i nie dłuższy niż rok z zaznaczeniem, że plan musi obejmować co najmniej jeden audyt.
3. Plan audytów IOD przygotowuje w formie rocznego harmonogramu i przedstawia Administratorowi Danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
4. W planie audytów IOD uwzględnia, w szczególności:
   - ❖ przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,
   - ❖ procesy przetwarzania danych osobowych objęte audytem,
   - ❖ konieczność weryfikacji zgodności przetwarzania danych osobowych z:
     - ▪ zasadami przetwarzania danych osobowych,
     - ▪ zasadami dotyczącymi zabezpieczenia danych osobowych,
     - ▪ zasadami przekazywania danych osobowych.
5. W toku audytu IOD dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
6. Po zakończeniu audytu, IOD przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
7. IOD przekazuje Administratorowi Danych sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.
8. Wzór sprawozdania z audytu stanowi załącznik nr 24 do Polityki.

9. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:
   - ❖ prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
   - ❖ prawo dostępu przysługujące osobie, której dane dotyczą (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),
   - ❖ prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).
2. Procedura realizacji praw osób, których dane dotyczą stanowi załącznik nr 18 do Polityki.
3. Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie zgodnie z art. 26 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi, bądź osobie upoważnionej przez pacjenta. Wniosek o udostępnienie dokumentacji medycznej stanowi załącznik nr 20 do Polityki, upoważnienie do wydania dokumentacji medycznej stanowi załącznik nr 21 do Polityki.

10. STOSOWANIE ZABEZPIECZEŃ WOBEC PRZETWARZANYCH DANYCH OSOBOWYCH

1. Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie wdraża odpowiednie środki techniczne i organizacyjne w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
   - ❖ stan wiedzy technicznej,
   - ❖ koszt wdrażania,
   - ❖ charakter, zakres, kontekst i cele przetwarzania danych,
   - ❖ ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
3. Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie wdraża takie środki techniczne i organizacyjne, mające na celu zapewnienie poufności, integralności oraz rozliczalności przetwarzanych danych osobowych, by przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.
4. Stosowane środki techniczne i organizacje muszą zapewnić, by dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5. Ogólny opis organizacyjnych środków bezpieczeństwa wdrożonych w strukturze Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie stanowi załącznik nr 15 do Polityki.
6. Ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie stanowi załącznik nr 16 do Polityki.

11. INCYDENTY OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych w przypadku naruszenia bezpieczeństwa przetwarzania danych zobowiązana jest do niezwłocznego poinformowania o tym fakcie Inspektora Ochrony Danych,
2. Na podstawie informacji, o których jest mowa w pkt. 1 Inspektor Ochrony Danych przeprowadza czynności wyjaśniające mające na celu zebranie informacji niezbędnych do podjęcia dalszych działań,
3. W przypadku stwierdzenia Incydentu, Inspektor Ochrony Danych Osobowych podejmuje działania doraźne takie jak:
   - ❖ czasowe odsunięcie pracownika od stanowiska pracy
   - ❖ zabezpieczenie miejsca w którym doszło do naruszenia
   - ❖ odłączenie komputera od sieci Internetu
   - ❖ zapewnienie bezpieczeństwa danym które były narażone
4. Procedura postępowania z incydentami ochrony danych osobowych stanowi załącznik nr 19 do Polityki.

12. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta*.
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
11. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.

12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.

13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym. Procedura bezpieczeństwa kluczy opisana jest w Instrukcji postępowania z kluczami i zabezpieczenie pomieszczeń, wydana Zarządzeniem 15/2021 z dnia 28 kwietnia 2021 roku Dyrektora WSPR w Olsztynie.

14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).

15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.

16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.

17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.

18. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

19. Celem sprawowania bieżącej kontroli oraz zapobieganiu naruszenia bezpieczeństwa danych osobowych Inspektor Ochrony Danych na podstawie danych od kierowników sekcji prowadzi analizę ryzyka. Wzór analizy ryzyka stanowi załącznik nr 24 do Polityki

13. PRZEGLĄDY I AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu Polityki dokonuje Inspektor Ochrony Danych
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
   - ❖ procesów funkcjonujących w strukturach Wojewódzkiej Stacji Pogotowia Ratunkowego w Olsztynie,
   - ❖ obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Wojewódzka Stacja Pogotowia Ratunkowego w Olsztynie.
4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Wojewódzkiej Stacji Pogotowia przegląd Polityki wykonywany jest niezwłocznie.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, Inspektor Ochrony Danych dokonuje aktualizacji Polityki w wymaganym zakresie.

14. ZAŁĄCZNIKI

Załącznik nr 1 - Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 2 - Wzór wniosku o nadanie upoważnienia

Załącznik nr 3 - Oświadczenie osoby upoważnionej

Załącznik nr 4 - Wzór rejestru nadanych upoważnień

Załącznik nr 5 - Wzór ewidencji nadanych uprawnień do systemów elektronicznych

Załącznik nr 6 - Zasady nadawania, zmiany i odwołania upoważnienia

Załącznik nr 7 - Rejestr czynności przetwarzania danych osobowych

Załącznik nr 8 - Rejestr kategorii przetwarzania danych osobowych

Załącznik nr 9 - Ewidencja zawartych umów powierzenia

Załącznik nr 10 - Protokół z usunięcia danych osobowych

Załącznik nr 11 - Obszar przetwarzania danych osobowych

Załącznik nr 12 - Wykaz zbiorów danych osobowych oraz systemów informatycznych

Załącznik nr 13 - Schemat przepływu danych

Załącznik nr 14 - Opis struktury zbiorów danych osobowych

Załącznik nr 15 - Ogólny opis zabezpieczeń organizacyjnych

Załącznik nr 16 - Ogólny opis zabezpieczeń technicznych

Załącznik nr 17 - Wzór umowy powierzenia

Załącznik nr 18 - Procedura realizacji praw osób, których dane osobowe dotyczą

Załącznik nr 19 - Procedura postępowania z incydentami

Załącznik nr 20 - Wniosek o udostępnienie dokumentacji medycznej

Załącznik nr 21 - Upoważnienie do wydania dokumentacji medycznej

Załącznik nr 22 - Procedura szkoleń

Załącznik nr 23 - Wzór sprawozdania z audytu

Załącznik nr 24 - Wzór analizy ryzyka

Dokument sporządzono:	**Podpis Administratora Danych:**	**Pieczęć**
Data: 30/04/2021 Miejsce: Olsztyn		